

Installationshandbuch

Revision A

McAfee® Email Gateway 7.0 – Virtual Appliance

Inhaltsverzeichnis

Einleitung

Dieses Handbuch enthält die Informationen, die Sie zum Installieren Ihres McAfee-Produkts benötigen.

Inhalt

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation von McAfee wird inhaltlich sorgfältig auf die Zielgruppe abgestimmt.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren** – Personen, die das Sicherheitsprogramm eines Unternehmens implementieren und umsetzen.

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel oder *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; Einführung eines neuen Begriffs; Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe` oder `Pfad`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; der Pfad eines Verzeichnisses oder Programms.
`Code`	Ein Code-Beispiel.
Benutzeroberfläche	Wörter aus der Benutzeroberfläche, einschließlich Optionen, Menüs, Schaltflächen und Dialogfeldern.
Hypertext-Blau	Ein funktionsfähiger Link auf ein Thema oder eine Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.



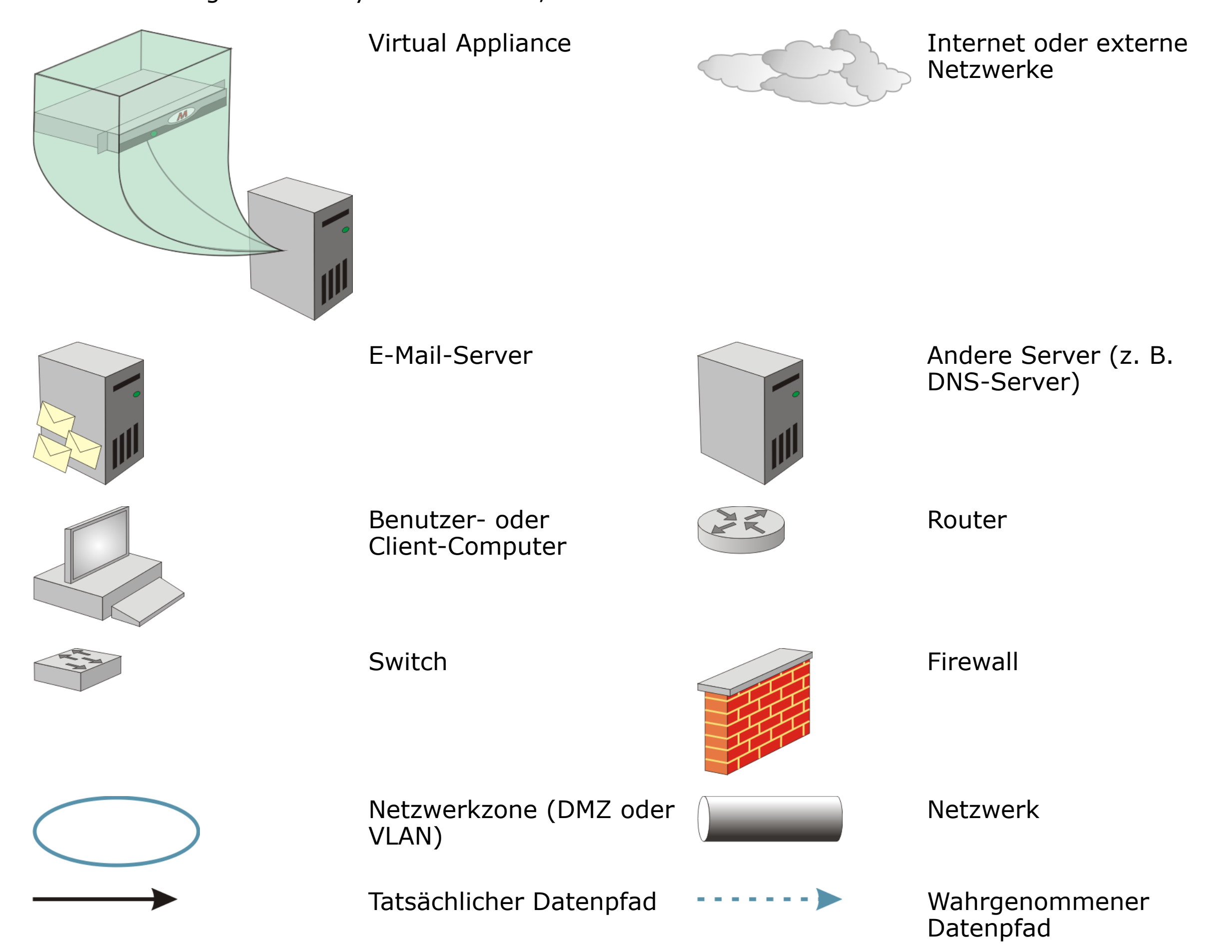
Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.



Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Graphische Konventionen

Lernen Sie die grafischen Symbole kennen, die in diesem Dokument verwendet werden.



Definition der Begriffe in diesem Handbuch

Lernen Sie einige der Schlüsselbegriffe kennen, die in diesem Dokument verwendet werden.

Begriff	Beschreibung
Demilitarisierte Zone (DMZ)	Ein Computer-Host oder kleineres Netzwerk, das als Puffer zwischen ein privates Netzwerk und das äußere öffentliche Netzwerk eingefügt wurde, um den direkten Zugriff durch außenstehende Benutzer auf Ressourcen im privaten Netzwerk zu verhindern.
DAT-Dateien	Erkennungsdefinitionsdateien (DAT), auch als Signaturdateien bezeichnet, enthalten die Definitionen, die Viren, Trojaner, Spyware, Adware und andere potenziell unerwünschte Programme (PUPe) identifizieren, erkennen und entfernen.
Betriebsmodus	Es gibt drei Betriebsmodi für das Produkt: "Expliziter Proxy", "Transparente Bridge" und "Transparenter Router".

Begriff	Beschreibung
Richtlinie	Eine Sammlung der Sicherheitskriterien (z. B. Konfigurationseinstellungen, Benchmarks und Spezifikationen für den Netzwerkzugriff), die die erforderliche Compliance-Stufe für Benutzer, Geräte und Systeme definieren, die von einer McAfee-Sicherheitsanwendung bewertet oder erzwungen werden kann.
Reputationsdienst-Prüfung	Teil der Absenderauthentifizierung. Wenn ein Absender die Reputationsdienst-Prüfung nicht besteht, ist die Appliance so eingestellt, dass die Verbindung beendet und die Nachricht nicht zugelassen wird. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und in Zukunft automatisch auf Kernel-Ebene blockiert.

Verwendung dieses Handbuchs

Dieser Abschnitt enthält eine kurze Zusammenfassung der in diesem Dokument enthaltenen Informationen.

In diesem Handbuch wird Folgendes behandelt:

- Planung und Ausführung Ihrer Installation.
- Umgang mit der Benutzeroberfläche.
- Testen der ordnungsgemäßen Funktion des Produkts.
- Anwendung der aktuellsten Erkennungsdefinitionsdateien.
- Vertrautmachen mit einigen Scan-Richtlinien, Erstellen von Berichten und Abrufen der Statusinformationen.
- Beheben einiger grundlegender Probleme.

Weitere Informationen über die Scan-Funktionen des Produkts finden Sie in der Online-Hilfe des Produkts und im *Administratorhandbuch zu McAfee Email Gateway 7.0*.

Quellen für Produktinformationen

McAfee stellt Ihnen die Informationen zur Verfügung, die Sie in den einzelnen Phasen der Produktimplementierung benötigen – von der Installation bis hin zur täglichen Nutzung und Fehlerbehebung. Nach der Produktveröffentlichung erhalten Sie Informationen zu diesem Produkt online in der KnowledgeBase von McAfee.

Vorgehensweise

1. Wechseln Sie zum McAfee Technical Support ServicePortal unter http://mysupport.mcafee.com.
2. Greifen Sie unter **Self Service** (Online-Support) auf den erforderlichen Informationstyp zu:

Zugriff auf	Vorgehensweise
Benutzerdokumentation	1 Klicken Sie auf **Product Documentation** (Produktdokumentation). 2 Wählen Sie ein Produkt und dann eine Version aus. 3 Wählen Sie ein Produktdokument aus.
KnowledgeBase	• Klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen), um Antworten auf Ihre produktbezogenen Fragen zu erhalten. • Klicken Sie auf **Browse the KnowledgeBase** (KnowledgeBase durchblättern), um Artikel nach Produkt und Version aufzulisten.

1 Einführung in McAfee Email Gateway Virtual Appliance

Die McAfee Email Gateway Virtual Appliance 7.0 bietet Unternehmen umfassenden Schutz gegen E-Mail-Bedrohungen in einer virtuellen Umgebung.

McAfee Email Gateway Virtual Appliance funktioniert in folgenden virtuellen Umgebungen:

- VMware vSphere 4.x
- VMware vSphere Hypervisor (ESXi) 4.x

Inhalt

Funktionen von McAfee E-Mail Gateway

Diese Informationen beschreiben die Funktionen des Produkts sowie deren Position in der Produktoberfläche.

E-Mail-Scan-Funktionen

Funktion	Beschreibung
Umfassender Scan-Schutz	Bietet Antiviren- und Anti-Spam-Schutz für die folgenden Netzwerkprotokolle: • SMTP • POP3
Antiviren-Schutz	**E-Mail | E-Mail-Richtlinien | Antivirus** Reduzierung der Bedrohungen für den gesamten Protokollverkehr durch folgende Mittel: • Virenschutzeinstellungen zur Identifizierung bekannter und unbekannter Bedrohungen von Viren in Archivdateien und anderen Dateitypen • Weitere Einstellungen für die Bedrohungserkennung zum Erkennen von Viren, potenziell unerwünschten Programmen, Komprimierungsprogrammen und anderer Malware • **Datei-Reputation von McAfee Global Threat Intelligence** zur Ergänzung der DAT-basierten Signaturen, indem den Appliances der Zugriff auf Millionen von Cloud-basierten Signaturen ermöglicht wird. Auf diese Weise wird der zeitliche Abstand zwischen der Erfassung einer neuen Malware-Bedrohung durch McAfee und deren Einbeziehung in DAT-Dateien reduziert und eine breitere Abdeckung gewährleistet.
Anti-Spam-Schutz	**E-Mail | E-Mail-Richtlinien | Spam** Verringert Spam in SMTP- und POP3-E-Mail-Verkehr durch folgende Mittel: • Anti-Spam-Modul, Anti-Spam- und Anti-Phishing-Regelsätze • Listen zugelassener und nicht zugelassener Absender • **E-Mail-Reputation von McAfee Global Threat Intelligence** zur Identifizierung von Absendern von Spam-E-Mails • Einschluss- und Ausschlusslisten, die Administratoren und Benutzer mithilfe eines Microsoft Outlook-Plug-Ins (nur auf Benutzerebene) erstellen können Erkennt Phishing-Angriffe und ergreift die entsprechenden Maßnahmen.

Funktion	Beschreibung
Verschlüsselung	**E-Mail | Verschlüsselung** Das McAfee Email Gateway umfasst mehrere Verschlüsselungsmethoden: • Server-zu-Server-Verschlüsselung • Secure Web Mail • Pull-Zustellung • Push-Zustellung Die Verschlüsselungsfunktionen können dafür eingerichtet werden, anderen Scan-Funktionen Verschlüsselungsdienste zur Verfügung zu stellen. Sie können jedoch auch als reine Verschlüsselungs-Server nur für die Verschlüsselung von E-Mails verwendet werden.
McAfee Global Threat Intelligence-Feedback	**E-Mail | E-Mail-Richtlinien | Richtlinienoptionen | McAfee GTI-Feedback** **System | Setup-Assistent** McAfee analysiert die Daten über Produkterkennungen und -warnmeldungen, Bedrohungsdetails und Nutzerstatistiken von einem vielschichtigen Kundenstamm, um wirksam gegen elektronische Angriffe vorzugehen, anfällige Systeme zu schützen und Internetkriminalität abzuwehren. Durch Ihre Teilnahme am Feedback-Dienst helfen Sie uns dabei, McAfee Global Threat Intelligence zu verbessern, sodass Ihre McAfee-Produkte effektiver arbeiten, und unterstützen unsere Zusammenarbeit mit Strafverfolgungsbehörden im Hinblick auf die Bekämpfung elektronischer Bedrohungen.
Compliance-Einstellungen	**E-Mail | E-Mail-Richtlinien | Compliance** Diese Version des Produkts beinhaltet Verbesserungen hinsichtlich der Art und Weise der Verwendung von Compliance-Regeln: • Verwenden Sie in der **Compliance**-Richtlinie den Assistenten für die Regelerstellung, um die integrierten Wörterbücher für die Compliance-Prüfung festzulegen, oder erstellen Sie eine neue Regel, für die Sie eine vorhandene Regel als Vorlage verwenden können. • Mit den Richtlinien **Mail-Größenfilterung** und **Dateifilterung** können Sie SMTP-E-Mail-Nachrichten auf echte Dateitypen überprüfen und auf der Grundlage der Größe und Anzahl der Anhänge Maßnahmen ergreifen.
Data Loss Prevention	**E-Mail | DLP und Compliance** Mit der **Data Loss Prevention**-Richtlinie können Sie kritische Dokumente hochladen und analysieren – dies wird als "Training" bezeichnet – und einen Fingerabdruck aller Dokumente erstellen.
Nachrichtensuche	**Berichte | Nachrichtensuche** Mit der Nachrichtensuche können Sie von einer einzigen Stelle der Benutzeroberfläche aus den Status von E-Mails bestätigen, die die Appliance durchlaufen haben. Sie erhalten Informationen zur E-Mail, beispielsweise ob sie zugestellt, blockiert, gebounct, isoliert oder in die Warteschlange für ausstehende weitere Aktionen gestellt wurde.

Funktion	Beschreibung
Quarantänefunktionen	**E-Mail | Quarantäne-Konfiguration | Quarantäneoptionen** • **Quarantäne-Digests** – Ermöglichen den Benutzern die Bearbeitung isolierter Elemente ohne Einbeziehung des E-Mail-Administrators. • **McAfee Quarantine Manager** – Fasst die Quarantäneverwaltung für McAfee-Produkte zusammen.
Message Transfer Agent	• Leitet Datenverkehr um, basierend auf Kriterien, die vom Administrator festgelegt werden. Beispielsweise können verschlüsselte E-Mails zur Entschlüsselung umgeleitet werden. • Erlaubt es dem Administrator, den finalen Status jeder Nachricht zu bestimmen. • Zeigt eine Kurzübersicht eingehender E-Mails nach Domänen, mit Detaillierungsmöglichkeiten nach Domäne und nicht zugestellter E-Mail nach Domäne. • Priorisiert die erneute Zustellung nicht zugestellter E-Mails abhängig von der Domäne. • Fasst die Zustellung mehrerer E-Mails an die jeweilige Domäne zusammen. • Erneutes Schreiben von E-Mail-Adressen bei ein- und ausgehender E-Mail auf der Grundlage normaler Ausdrücke, die vom Administrator definiert wurden. • Entfernt E-Mail-Header bei ausgehenden Nachrichten, um den Aufbau der internen Netzwerkinfrastruktur zu verbergen. • Versendet E-Mails unter Verwendung von TLS. • Verwaltet Zertifikate.

Berichterstellungs- und Systemfunktionen

Funktion	Beschreibung
Geplante Berichte	**Berichte | Geplante Berichte** Sie können Berichte planen, die regelmäßig ausgeführt und an einen oder mehrere E-Mail-Empfänger gesendet werden sollen.
Protokollierungsoptionen	**System | Protokollierung, Warnung und SNMP** Sie können die Appliance für das Senden von E-Mails, die Informationen zu Viren und anderen erkannten Bedrohungen enthalten, sowie für die Verwendung von SNMP zum Übertragen von Informationen von der Appliance konfigurieren.
Dashboard-Statistiken	**Dashboard** Das Dashboard bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Aktivitäten der Appliance ansehen können, wie beispielsweise von der Appliance verarbeitete E-Mails und den Gesamtsystemstatus der Appliance. Sie können auch direkt zu den Bereichen der Benutzeroberfläche wechseln, die Sie häufig verwenden.

Funktion	Beschreibung
Verwalten von Appliances über ePolicy Orchestrator	**System | Setup-Assistent** Wählen Sie die Option **Einrichten der Verwaltung durch ePO**, um den Status Ihrer Appliances zu überwachen und Ihre Appliance von ePolicy Orchestrator aus zu verwalten. Sie können die Appliances direkt über ePolicy Orchestrator verwalten, ohne die Benutzeroberfläche für jede Appliance starten zu müssen. In ePolicy Orchestrator ähneln die Seiten der Benutzeroberfläche, die Sie zum Konfigurieren und Verwalten Ihrer Appliance verwenden, hinsichtlich ihrer Gestaltung den Seiten, die Sie von den Appliances gewohnt sind.
Cluster-Verwaltung	**System | Systemverwaltung | Cluster-Verwaltung** Die Cluster-Verwaltung ermöglicht Ihnen, Gruppen von zusammenarbeitenden Appliances einzurichten, um die Scan-Arbeitslast zu verteilen und für den Fall eines Hardware-Fehlers Redundanz zu bieten. Auf diesen Seiten können Sie Ihre Konfigurationen sichern und wiederherstellen, Konfigurationen von einer Appliance auf andere Appliances übertragen und den Lastenausgleich zwischen den Appliances einrichten.
Virtuelle Hosts	**System | Virtuelles Hosting | Virtuelle Hosts** Für das SMTP-Protokoll können Sie im Adresspool für eingehenden Datenverkehr die Adressen angeben, an denen die Appliance Datenverkehr empfängt oder abfängt. Unter Verwendung virtueller Hosts kann eine einzelne Appliance sich wie verschiedene Appliances verhalten. Jede Appliance kann Datenverkehr innerhalb angegebener IP-Adresspools verwalten, wodurch die Appliance Scan-Dienste für Datenverkehr von zahlreichen Kunden bieten kann.
Rollenbasierte Zugriffskontrolle	**System | Benutzer | Benutzer und Rollen** **System | Benutzer | Anmeldedienste** Zusätzlich zur Kerberos-Authentifizierungsmethode steht auch die RADIUS-Authentifizierung zur Verfügung.

Umfang des Download-Pakets

McAfee Email Gateway Virtual Appliance 7.0 wird in einer ZIP-Datei zur Verfügung gestellt, die die Software-Installationsdateien und Installationsdokumente zur Installation der virtuellen Appliance auf VMware vSphere 4.x enthält.



Das Download-Paket enthält keine Installationsdateien für das VMware-Produkt. Wenn Sie Ihre virtuelle Software noch nicht eingerichtet haben, gehen Sie zur VMware-Website (http://www.vmware.com), um VMware vSphere oder VMware vSphere Hypervisor (ESXi) zu erwerben.

2 Vorbereitung der Installation

Um den sicheren Betrieb des McAfee Email Gateway Virtual Appliance 7.0 zu gewährleisten, beachten Sie Folgendes, bevor Sie mit der Installation beginnen.

- Machen Sie sich mit den Betriebsmodi und den Funktionen vertraut. Es ist wichtig, dass Sie eine gültige Konfiguration auswählen.
- Entscheiden Sie, wie Sie die Appliance in Ihr Netzwerk integrieren möchten, und stellen Sie fest, welche Informationen Sie benötigen, bevor Sie beginnen. Sie benötigen beispielsweise den Namen und die IP-Adresse des Geräts.

Inhalt

Nicht bestimmungsgemäße Nutzung

Erfahren Sie, wie Sie vermeiden, das Produkt nicht bestimmungsgemäß zu nutzen.

McAfee Email Gateway Virtual Appliance 7.0 ist:

- **Keine Firewall** – Es muss in Ihrer Organisation hinter einer ordnungsgemäß konfigurierten Firewall verwendet werden.
- **Kein Server zum Speichern zusätzlicher Software und Dateien** – Installieren Sie keine Software auf dem Gerät, und fügen Sie keine zusätzlichen Dateien hinzu, es sei denn, Sie werden in der Produktdokumentation oder von Ihrem Support-Mitarbeiter dazu aufgefordert.



Das Gerät kann nicht alle Arten von Datenverkehr verarbeiten. Wenn Sie den Modus "Expliziter Proxy" verwenden, sollten nur Protokolle an das Gerät gesendet werden, die gescannt werden müssen.

Überlegungen zu Netzwerkmodi

In diesem Abschnitt lernen Sie die Betriebsmodi (Netzwerkmodi) kennen, in denen das Gerät betrieben werden kann.

Bevor Sie das McAfee Email Gateway konfigurieren, müssen Sie sich überlegen, welchen Netzwerkmodus Sie verwenden möchten. Vom ausgewählten Modus hängt es ab, wie Sie Ihren **VMware ESX**-Host physisch an Ihr Netzwerk anschließen. Verschiedene Modi wirken sich auch auf die Konfiguration Ihres vSwitch aus, an den Ihre virtuelle Appliance angeschlossen wird. Die Ausführung der virtuellen Appliance im Modus "Expliziter Proxy" erfordert den geringsten Konfigurationsaufwand

auf dem VMware ESX-Host und ist leichter einzurichten. Für die Installation der virtuellen Appliance in einem der transparenten Modi müssen andere Überlegungen getroffen werden. Im Folgenden werden alle erforderlichen Schritte für die ESX-Konfiguration in einem der beiden Modi beschrieben.

Sie können einen der folgenden Netzwerkmodi auswählen:

- **Modus "Expliziter Proxy"** – Die virtuelle Appliance fungiert als Proxyserver und Mail-Relay.
- **Modus "Transparenter Router"** – Die virtuelle Appliance fungiert als Router.
- **Modus "Transparente Bridge"** – Die virtuelle Appliance fungiert als Ethernet-Bridge.

Wenn Sie nach der Lektüre dieses und der folgenden Abschnitte weiterhin unsicher sind, welchen Modus Sie verwenden sollen, sprechen Sie mit einem Netzwerkexperten.

Modus "Expliziter Proxy"

In diesem Abschnitt lernen Sie den Modus "Expliziter Proxy" des McAfee Email Gateways besser kennen.

Im Modus "Expliziter Proxy" müssen einige Netzwerkgeräte so eingerichtet werden, dass sie Datenverkehr explizit an das Gerät senden. Das Gerät fungiert dann als Proxy oder Relay und verarbeitet den Datenverkehr für die Geräte.

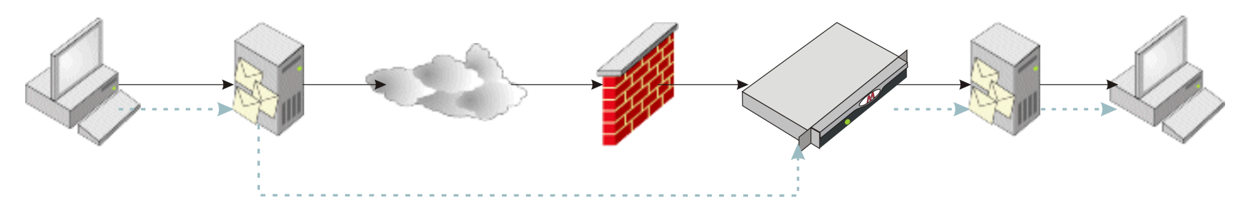


Abbildung 2-1 Modus "Expliziter Proxy" – sichtbarer Datenpfad

Der Modus "Expliziter Proxy" ist am besten für Netzwerke geeignet, in denen Client-Geräte über ein einzelnes Upstream- und Downstream-Gerät eine Verbindung zum Gerät herstellen.



Dies ist möglicherweise nicht die beste Option, wenn verschiedene Netzwerkgeräte erneut konfiguriert werden müssen, damit sie den Datenverkehr an das Gerät senden.

Netzwerk- und Gerätekonfiguration

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet, müssen Sie den internen Mail-Server explizit so konfigurieren, dass er E-Mail-Verkehr an das Gerät sendet. Das Gerät prüft den E-Mail-Verkehr, bevor es ihn im Namen des Absenders an den externen Mail-Server weiterleitet. Der externe E-Mail-Server leitet die E-Mail dann an den Empfänger weiter.

Entsprechend muss das Netzwerk so konfiguriert werden, dass eingehende E-Mail-Nachrichten aus dem Internet nicht dem internen Mail-Server, sondern dem Gerät zugestellt werden.

Das Gerät kann den E-Mail-Verkehr dann prüfen, bevor es ihn im Namen des Absenders an den internen E-Mail-Server zur Zustellung weiterleitet, wie in der Abbildung dargestellt.

Beispielsweise kann ein externer Mail-Server direkt mit dem Gerät kommunizieren, auch wenn der Datenverkehr möglicherweise mehrere Netzwerkserver passiert, bevor er das Gerät erreicht. Der wahrgenommene Pfad verläuft vom externen Mail-Server zum Gerät.

Protokolle

Um ein unterstütztes Protokoll zu scannen, müssen Sie Ihre anderen Netzwerkserver oder Client-Computer so konfigurieren, dass das Protokoll durch das Gerät geleitet wird, sodass kein Datenverkehr das Gerät umgehen kann.

Firewall-Regeln

Im Modus "Expliziter Proxy" werden alle Firewall-Regeln, die für den Client-Zugriff auf das Internet eingerichtet wurden, außer Kraft gesetzt. Für die Firewall sind nur die physischen IP-Adressinformationen für das Gerät sichtbar, nicht jedoch die IP-Adressen der Clients. Die Firewall kann daher ihre Internetzugriffsregeln nicht auf die Clients anwenden.

Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr vom McAfee® Email Gateway akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt.

Richten Sie Firewall-Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Platzieren des Geräts

Konfigurieren Sie die Netzwerkgeräte so, dass der zu scannende Datenverkehr an das McAfee® Email Gateway gesendet wird. Das ist wichtiger als der Standort des McAfee® Email Gateway.

Der Router muss allen Benutzern erlauben, eine Verbindung zum McAfee® Email Gateway herzustellen.

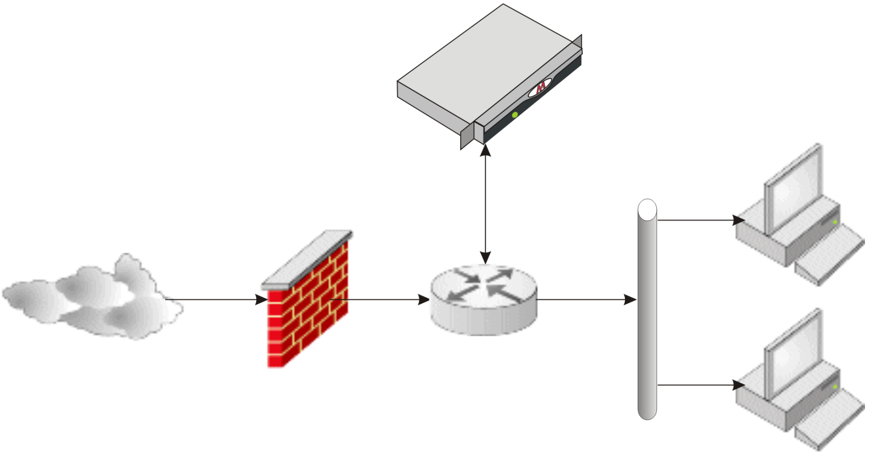


Abbildung 2-2 Platzierung im Modus "Expliziter Proxy"

Das McAfee® Email Gateway muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden, wie in Abbildung 6 dargestellt: Konfiguration als expliziter Proxy.

Normalerweise ist die Firewall so konfiguriert, dass der Datenverkehr, der nicht direkt von dem Gerät stammt, gesperrt wird. Wenn Sie in Bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkspezialisten.

Verwenden Sie diese Konfiguration in folgenden Fällen:

- Das Gerät wird im Modus "Expliziter Proxy" betrieben.
- Sie verwenden E-Mail (SMTP).

Für diese Konfiguration gilt:

- Konfigurieren Sie die externen DNS-Server (Domain Name System) oder NAT (Network Address Translation) auf der Firewall so, dass der externe Mail-Server E-Mails an das Gerät zustellt, nicht an den internen Mail-Server.
- Konfigurieren Sie die internen Mail-Server so, dass E-Mail-Verkehr an das Gerät gesendet wird. Das heißt, die internen Mail-Server müssen das Gerät als Smart-Host verwenden. Vergewissern Sie sich, dass die Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.
- Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr von dem Gerät akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt. Richten Sie Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Modus "Transparente Bridge"

In diesem Abschnitt lernen Sie den Modus "Transparente Bridge" des McAfee Email Gateways besser kennen.

Im Modus "Transparente Bridge" bemerken die kommunizierenden Server das Gerät nicht. Der Betrieb des Geräts ist für die Server transparent.

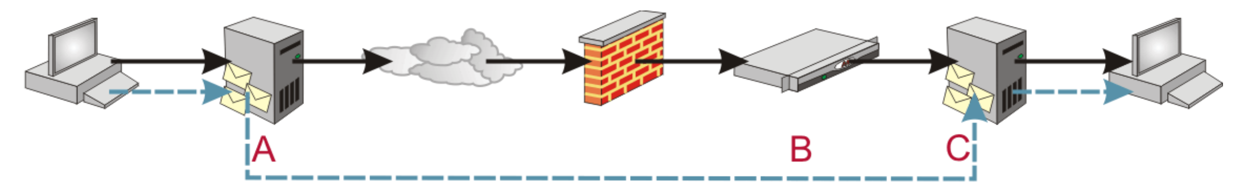


Abbildung 2-3 Modus "Transparente Bridge" – sichtbarer Datenpfad

In der Abbildung sendet der externe E-Mail-Server (**A**) E-Mail-Nachrichten an den internen E-Mail-Server (**C**). Der externe Mail-Server kann nicht erkennen, dass die von ihm gesendete E-Mail-Nachricht vom Gerät abgefangen und gescannt wird (**B**).

Der externe E-Mail-Server scheint direkt mit dem internen E-Mail-Server zu kommunizieren (der Pfad wird als gestrichelte Linie dargestellt). Tatsächlich wird der Datenverkehr möglicherweise durch mehrere Netzwerkgeräte geleitet und vom Gerät abgefangen und gescannt, bevor er den internen Mail-Server erreicht.

Arbeitsweise des Geräts im Modus "Transparente Bridge"

Im Modus "Transparente Bridge" wird das Gerät über den LAN1- und den LAN2-Anschluss mit dem Netzwerk verbunden. Das Gerät scannt den empfangenen Datenverkehr und fungiert als Bridge, die zwei Netzwerksegmente verbindet, behandelt diese aber wie ein einziges logisches Netzwerk.

Konfiguration im Modus "Transparente Bridge"

Der Modus "Transparente Bridge" erfordert weniger Konfigurationsaufwand als die Modi "Transparenter Router" oder "Expliziter Proxy". Sie müssen nicht alle Clients, das Standard-Gateway, MX-Einträge, Firewall-NAT und E-Mail-Server neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Da das Gerät in diesem Modus nicht als Router fungiert, ist es auch nicht erforderlich, eine Routing-Tabelle zu aktualisieren.

Platzieren des Geräts bei Betrieb im Modus "Transparente Bridge"

Aus Sicherheitsgründen sollten Sie das Gerät innerhalb Ihres Unternehmens und hinter einer Firewall betreiben.

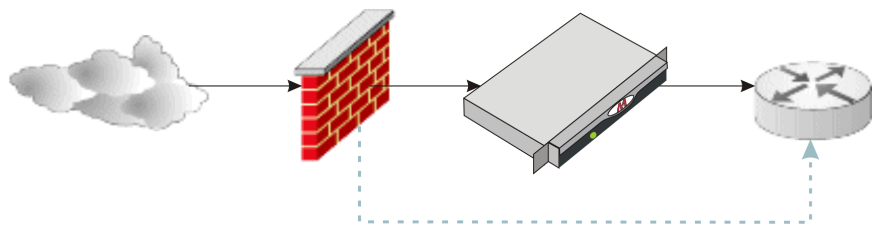


Abbildung 2-4 Platzierung im Modus "Transparente Bridge"



Platzieren Sie das Gerät im Modus "Transparente Bridge" zwischen der Firewall und Ihrem Router, wie in der Abbildung dargestellt.

In diesem Modus verbinden Sie zwei Netzwerksegmente physisch mit dem Gerät. Das Gerät behandelt diese als eine einzige logische Einheit. Da sich die Geräte – Firewall, Gerät und Router – im selben logischen Netzwerk befinden, müssen sie kompatible IP-Adressen im selben Subnetz haben.

Geräte auf der einen Seite der Bridge (z. B. ein Router), die mit den Geräten auf der anderen Seite der Bridge (z. B. einer Firewall) kommunizieren, bemerken die Bridge nicht. Sie erkennen nicht, dass der Datenverkehr abgefangen und gescannt wird. Deshalb wird dieser Betriebsmodus des Geräts als "Transparente Bridge" bezeichnet.

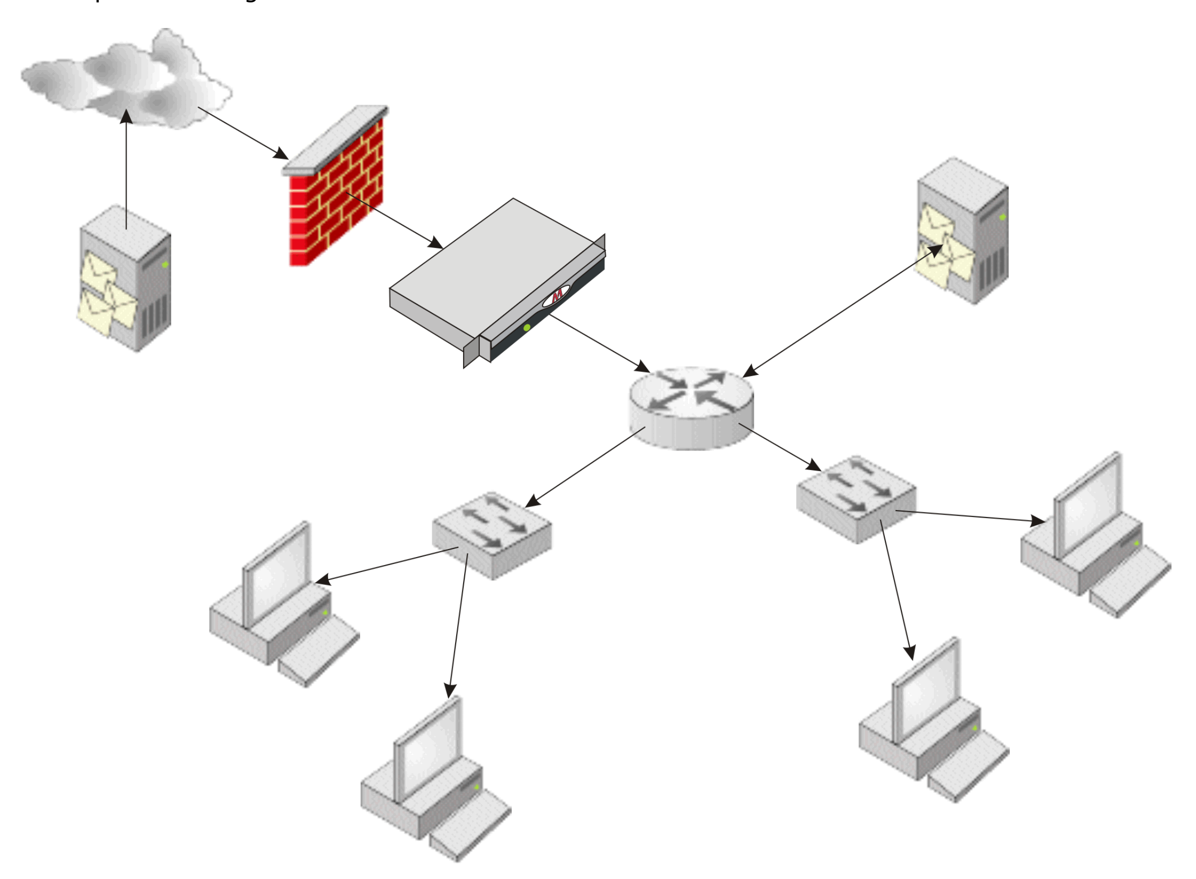


Abbildung 2-5 Netzwerkstruktur – Modus "Transparente Bridge"

Modus "Transparenter Router"

In diesem Abschnitt lernen Sie den Modus "Transparenter Router" des McAfee Email Gateways besser kennen.

Im Modus "Transparenter Router" scannt das Gerät den E-Mail-Verkehr zwischen zwei Netzwerken. Das Gerät hat eine IP-Adresse für ausgehenden gescannten Verkehr und muss eine IP-Adresse für eingehenden Verkehr haben.

Die kommunizierenden Netzwerkserver erkennen nicht, dass das Gerät zwischengeschaltet ist. Der Betrieb des Geräts ist für die Geräte transparent.

Arbeitsweise des Geräts im Modus "Transparente Router"

Im Modus "Transparenter Router" wird das Gerät mit den Netzwerken über den LAN1- und den LAN2-Anschluss verbunden. Das Gerät scannt den Datenverkehr, der über ein Netzwerk eingeht, und leitet ihn an das nächste Netzwerkgerät in einem anderen Netzwerk weiter. Das Gerät fungiert als Router (wobei es Datenverkehr zwischen den verschiedenen Netzwerken auf der Basis der Informationen in den Routing-Tabellen weiterleitet).

Konfiguration im Modus "Transparenter Router"

Im Modus "Transparenter Router" müssen Sie Ihre Netzwerkgeräte nicht explizit neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Sie müssen lediglich die Routing-Tabelle für das Gerät konfigurieren und einige der Routing-Informationen für die Netzwerkgeräte auf einer Seite des Geräts ändern (der Geräte also, die an die LAN1- und LAN2-Anschlüsse des Geräts angeschlossen sind). Es könnte zum Beispiel erforderlich sein, das Gerät als Standard-Gateway zu konfigurieren.

Im Modus "Transparenter Router" muss das Gerät zwei Netzwerke miteinander verbinden. Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden.



Im Modus "Transparenter Router" werden weder Multicast-IP-Datenverkehr noch andere Protokolle wie NETBEUI und IPX (Nicht-IP-Protokolle) unterstützt.

Firewall-Regeln

Im Modus "Transparenter Router" wird die Firewall mit der physischen IP-Adresse für die LAN1/ LAN2-Verbindung mit dem Management-Blade-Server verbunden.

Platzieren des Geräts

Verwenden Sie das Gerät im Modus "Transparenter Router", um einen im Netzwerk vorhandenen Router zu ersetzen.



Wenn Sie den Modus "Transparenter Router" verwenden und keinen vorhandenen Router ersetzen, müssen Sie einen Teil Ihres Netzwerks neu konfigurieren, damit der Datenverkehr korrekt durch das Gerät fließt.

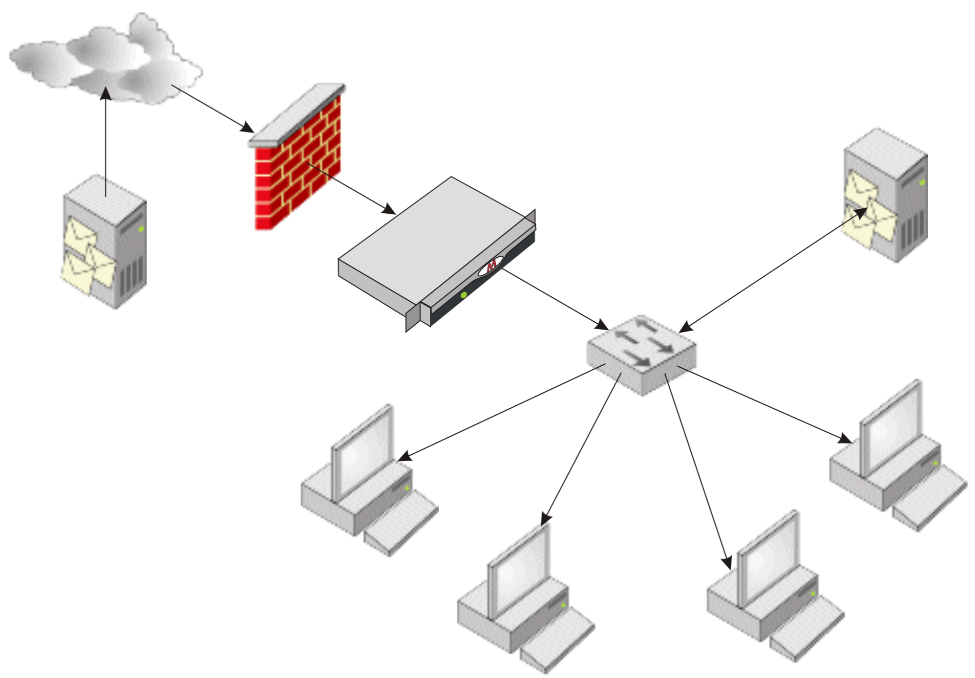


Abbildung 2-6 Netzwerkstruktur – Modus "Transparente Bridge"

Sie müssen wie folgt vorgehen:

- Konfigurieren Sie die Client-Geräte so, dass sie auf das Standard-Gateway verweisen.
- Konfigurieren Sie das Gerät so, dass das Internet-Gateway als Standard-Gateway verwendet wird.
- Stellen Sie sicher, dass Ihre Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.

Netzwerkkonfiguration für VMware vSphere

Diese Gruppe von Aufgaben stellt dar, wie Sie Ihre vSwitch-Konfiguration für die möglichen Betriebsmodi vorbereiten.

Vorgehensweise – Konfigurieren von VMware vSphere für eine Installation im Modus "Expliziter Proxy"

Gehen Sie wie nachfolgend beschrieben vor, um VMware vSphere so zu konfigurieren, dass die virtuelle Appliance im Modus "Expliziter Proxy"installiert wird.

Bevor Sie beginnen

Stellen Sie sicher, dass auf Ihrem VMware ESX-Host mindestens zwei verschiedene physische Schnittstellen zur Verfügung stehen. Eine dritte Schnittstelle kann für die Out-of-band-Verwaltung verwendet werden.

Aus Gründen der Leistungsoptimierung empfiehlt McAfee, die von der virtuellen Maschine mit McAfee Email Gateway Virtual Appliance verwendeten Schnittstellen nicht von anderen virtuellen Maschinen auf diesem VMware ESX-Host nutzen zu lassen. Bevor Sie mit der

Installation der virtuellen Appliance beginnen, müssen vSwitches erstellt worden sein, die mit LAN 1 und LAN 2 der virtuellen Appliance verbunden werden können und die ordnungsgemäß konfiguriert sind.

Wenn Sie die .OVA-Datei für McAfee Email Gateway Virtual Appliance importieren, stellen Sie sicher, dass die **LAN-1**-Schnittstelle mit dem ersten vSwitch und die **LAN-2**-Schnittstelle mit dem zweiten vSwitch verbunden ist.



Sie müssen auf jedem Host im Hochverfügbarkeits-Cluster (High Availability, HA) identische vSwitches erstellen, falls VMotion eingesetzt wird.

Vorgehensweise

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie im linken Bereich der Ansicht **Hosts and Clusters** (Hosts und Cluster) den Host aus, auf dem Sie die virtuelle Appliance installieren möchten.
3. Wählen Sie auf der rechten Seite **Configuration** (Konfiguration).
4. Klicken Sie auf **Networking** (Netzwerk).
5. Klicken Sie auf **Add Networking** (Netzwerk hinzufügen).
6. Wählen Sie im Assistenten **Add Network** (Netzwerk hinzufügen) **Virtual Machine** (Virtuelle Maschine) aus, und klicken Sie auf **Next** (Weiter).
7. Wählen Sie **Create a virtual switch** (Virtuellen Switch erstellen), wählen Sie die physische Schnittstelle aus, die Sie für die LAN-1-Verbindung der virtuellen Appliance verwenden möchten, und klicken Sie auf **Next** (Weiter).
8. Geben Sie eine Bezeichnung für Ihr neues Netzwerk ein, z. B. `MEG LAN 1`.
9. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertig stellen).
10. Wiederholen Sie die Schritte 5 bis 10, um einen zweiten vSwitch für die LAN-2-Schnittstelle hinzuzufügen.

Vorgehensweise – Konfigurieren von VMware vSphere für eine Installation im Modus "Transparente Bridge"

Gehen Sie wie nachfolgend beschrieben vor, um VMware vSphere so zu konfigurieren, dass die virtuelle Appliance im Modus "Transparente Bridge" installiert wird.

Bevor Sie beginnen

Stellen Sie sicher, dass auf Ihrem VMware ESX-Host mindestens zwei verschiedene physische Schnittstellen zur Verfügung stehen. Die beiden Schnittstellen, die für die Bridge verwendet werden, müssen mit verschiedenen Broadcast-Domänen verbunden sein, um Netzwerk-Loops zu vermeiden, die schwerwiegende Störungen in Ihrem Netzwerk verursachen könnten. Eine dritte Schnittstelle kann für die Out-of-band-Verwaltung verwendet werden.

Aus Gründen der Leistungsoptimierung empfiehlt McAfee, die von der Bridge verwendeten Schnittstellen der virtuellen Maschine mit McAfee Email Gateway Virtual Appliance dediziert zuzuordnen und nicht von anderen virtuellen Maschinen auf diesem VMware ESX-Host nutzen zu lassen. Bevor Sie mit der Installation der virtuellen Appliance beginnen, müssen vSwitches erstellt worden sein, die mit LAN 1 und LAN 2 der virtuellen Appliance verbunden werden können und die ordnungsgemäß konfiguriert sind.

Wenn Sie die .OVA-Datei für McAfee Email Gateway Virtual Appliance importieren, stellen Sie sicher, dass die **LAN-1**-Schnittstelle mit dem ersten vSwitch und die **LAN-2**-Schnittstelle mit dem zweiten vSwitch verbunden ist.



Sie müssen auf jedem Host im Hochverfügbarkeits-Cluster (High Availability, HA) identische vSwitches erstellen, falls VMotion eingesetzt wird.

Vorgehensweise

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie im linken Bereich der Ansicht **Hosts and Clusters** (Hosts und Cluster) den Host aus, auf dem Sie die virtuelle Appliance installieren möchten.
3. Wählen Sie auf der rechten Seite **Configuration** (Konfiguration).
4. Klicken Sie auf **Networking** (Netzwerk).
5. Klicken Sie auf **Add Networking** (Netzwerk hinzufügen).
6. Wählen Sie im Assistenten **Add Network** (Netzwerk hinzufügen) **Virtual Machine** (Virtuelle Maschine) aus, und klicken Sie auf **Next** (Weiter).
7. Wählen Sie **Create a virtual switch** (Virtuellen Switch erstellen), wählen Sie die physische Schnittstelle aus, die Sie für die LAN-1-Verbindung der virtuellen Appliance verwenden möchten, und klicken Sie auf **Next** (Weiter).
8. Geben Sie eine Bezeichnung für Ihr neues Netzwerk ein, z. B. `MEG LAN 1`.

   Standardmäßig entfernt VMware ESX VLAN-Tags. Damit die virtuelle Appliance den für das VLAN gekennzeichneten Datenverkehr sehen kann (beispielsweise für das Erstellen VLAN-spezifischer Richtlinien), müssen Sie **Virtual Guest Tagging** aktivieren. Weitere Informationen hierzu finden Sie im Artikel 1004252 der VMware Knowledge Base.

9. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertig stellen).
10. Blättern Sie auf der Seite nach unten zu dem virtuellen Switch, den Sie gerade erstellt haben, und klicken Sie auf **Properties** (Eigenschaften).
11. Doppelklicken Sie in **vSwitch Properties** (vSwitch-Eigenschaften) links in der Liste auf den Eintrag **vSwitch**.
12. Klicken Sie auf **Security** (Sicherheit).
13. Ändern Sie den Wert im Feld **Promiscuous Mode** (Promiscuous-Modus) in **Accept** (Akzeptieren), und klicken Sie auf **OK**.
14. Klicken Sie auf **Schließen**.
15. Wiederholen Sie die Schritte 5 bis 14, um einen zweiten vSwitch für die LAN-2-Schnittstelle hinzuzufügen.

   Die zweite vSwitch muss mit einer anderen physischen Schnittstelle verbunden werden, die ihrerseits mit einer anderen Broadcast-Domäne in Ihrem Netzwerk verbunden sein muss, als es die für den ersten vSwitch verwendete Schnittstelle ist.

Vorgehensweise – Konfigurieren von VMware vSphere für eine Installation im Modus "Transparenter Router"

Gehen Sie wie nachfolgend beschrieben vor, um VMware vSphere so zu konfigurieren, dass die virtuelle Appliance im Modus "Transparenter Router" installiert wird.

Bevor Sie beginnen

Stellen Sie sicher, dass auf Ihrem VMware ESX-Host mindestens zwei verschiedene physische Schnittstellen zur Verfügung stehen. Eine dritte Schnittstelle kann für die Out-of-band-Verwaltung verwendet werden.

Aus Gründen der Leistungsoptimierung empfiehlt McAfee, die von der virtuellen Maschine mit McAfee Email Gateway Virtual Appliance verwendeten Schnittstellen nicht von anderen virtuellen Maschinen auf diesem VMware ESX-Host nutzen zu lassen. Bevor Sie mit der Installation der virtuellen Appliance beginnen, müssen vSwitches erstellt worden sein, die mit LAN 1 und LAN 2 der virtuellen Appliance verbunden werden können und die ordnungsgemäß konfiguriert sind.

Wenn Sie die .OVA-Datei für McAfee Email Gateway Virtual Appliance importieren, stellen Sie sicher, dass die **LAN-1**-Schnittstelle mit dem ersten vSwitch und die **LAN-2**-Schnittstelle mit dem zweiten vSwitch verbunden ist.



Sie müssen auf jedem Host im Hochverfügbarkeits-Cluster (High Availability, HA) identische vSwitches erstellen, falls VMotion eingesetzt wird.

Vorgehensweise

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie im linken Bereich der Ansicht **Hosts and Clusters** (Hosts und Cluster) den Host aus, auf dem Sie die virtuelle Appliance installieren möchten.
3. Wählen Sie auf der rechten Seite **Configuration** (Konfiguration).
4. Klicken Sie auf **Networking** (Netzwerk).
5. Klicken Sie auf **Add Networking** (Netzwerk hinzufügen).
6. Wählen Sie im Assistenten **Add Network** (Netzwerk hinzufügen) **Virtual Machine** (Virtuelle Maschine) aus, und klicken Sie auf **Next** (Weiter).
7. Wählen Sie **Create a virtual switch** (Virtuellen Switch erstellen), wählen Sie die physische Schnittstelle aus, die Sie für die LAN-1-Verbindung der virtuellen Appliance verwenden möchten, und klicken Sie auf **Next** (Weiter).
8. Geben Sie eine Bezeichnung für Ihr neues Netzwerk ein, z. B. `MEG LAN 1`.
9. Klicken Sie auf **Next** (Weiter) und anschließend auf **Finish** (Fertig stellen).
10. Wiederholen Sie die Schritte 5 bis 10, um einen zweiten vSwitch für die LAN-2-Schnittstelle hinzuzufügen.

    Der zweite vSwitch muss mit einer anderen als der für Ihren ersten vSwitch verwendeten physischen Schnittstelle verbunden werden.

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ

Lernen Sie demilitarisierte Zonen in Ihrem Netzwerk kennen, und erfahren Sie, wie Sie diese zum Schutz Ihrer E-Mail-Server verwenden können.

Eine "demilitarisierte Zone" (Demilitarized Zone, DMZ) ist ein Netzwerk, das durch eine Firewall von allen anderen Netzwerken getrennt ist, auch vom Internet und anderen internen Netzwerken. Eine DMZ wird üblicherweise mit dem Ziel implementiert, den Zugriff auf Server zu sperren, die Internetdienste (beispielsweise E-Mail) zur Verfügung stellen.

Hacker verschaffen sich oft Zugriff auf Netzwerke, indem sie herausfinden, auf welchen TCP-/UDP-Ports Appliances Anfragen erwarten, und dann bekannte Schwachstellen in Appliances ausnutzen. Firewalls senken das Risiko solcher Exploits erheblich, indem sie den Zugriff auf bestimmte Ports auf bestimmten Servern steuern.

Das Gerät kann einfach zu einer DMZ-Konfiguration hinzugefügt werden. Die Art, wie Sie das Gerät in einer DMZ verwenden, hängt von den zu scannenden Protokollen ab.

SMTP-Konfiguration in einer DMZ

Erfahren Sie, wie Sie SMTP-Geräte, die sich innerhalb einer demilitarisierten Zone Ihres Netzwerks befinden, konfigurieren.

Die DMZ ist eine gute Möglichkeit für das Verschlüsseln von E-Mails. Wenn der E-Mail-Verkehr die Firewall zum zweiten Mal erreicht (auf seinem Weg von der DMZ zum Internet), ist er verschlüsselt.

Geräte, die SMTP-Verkehr in einer DMZ scannen können, sind normalerweise im Modus "Expliziter Proxy" konfiguriert.

Konfigurationsänderungen müssen nur an den MX-Einträgen für die E-Mail-Server vorgenommen werden.



HINWEIS: Sie können den Modus "Transparente Bridge" verwenden, wenn Sie SMTP in einer DMZ scannen. Wenn Sie jedoch den Datenfluss nicht richtig steuern, scannt das Gerät jede Nachricht zweimal, einmal in jede Richtung. Aus diesem Grund wird für SMTP-Scans normalerweise der Modus "Expliziter Proxy" verwendet.

E-Mail-Relay

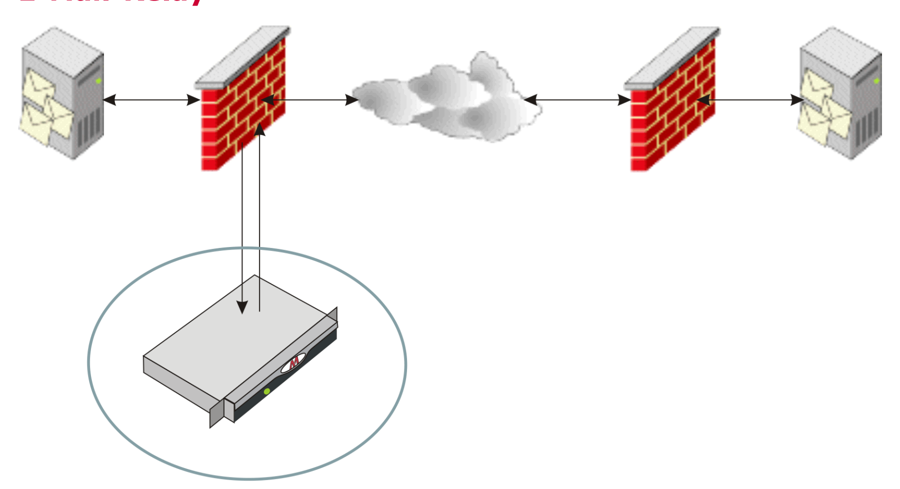


Abbildung 2-7 Konfigurieren als Mail-Relay

Wenn Sie in Ihrer DMZ bereits ein Relay eingerichtet haben, können Sie es durch das Gerät ersetzen.

Um Ihre bestehenden Firewall-Richtlinien zu verwenden, geben Sie dem Gerät dieselbe IP-Adresse wie dem Mail-Relay.

E-Mail-Gateway

SMTP bietet keine Methoden zur Verschlüsselung von E-Mail-Nachrichten. Sie können mithilfe von TLS (Transport Layer Security) den Link verschlüsseln, nicht jedoch die E-Mail-Nachrichten. Daher erlauben einige Unternehmen solchen Datenverkehr nicht in ihrem internen Netzwerk. Zur Umgehung dieses Problems wird häufig ein proprietäres E-Mail-Gateway eingesetzt, zum Beispiel Lotus Notes® oder Microsoft® Exchange, um den E-Mail-Datenverkehr zu verschlüsseln, bevor er das Internet erreicht.

Um eine DMZ-Konfiguration unter Verwendung des proprietären E-Mail-Gateways zu implementieren, fügen Sie das Scan-Gerät zur DMZ auf der SMTP-Seite des Gateways hinzu.

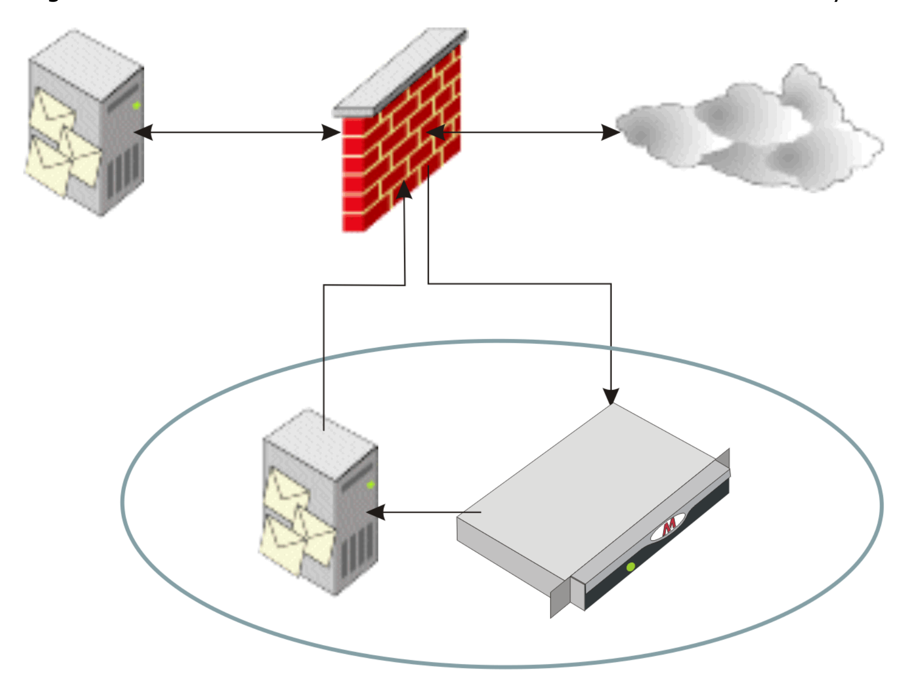


Abbildung 2-8 Konfigurieren als E-Mail-Gateway

Nehmen Sie hierfür folgende Konfigurationen vor:

- Die öffentlichen MX-Einträge müssen externe Mail-Server anweisen, alle eingehenden E-Mail-Nachrichten an das Gerät (statt an das Gateway) zu senden.
- Das Gerät muss alle eingehenden E-Mail-Nachrichten an das Mail-Gateway und alle ausgehenden Nachrichten per DNS oder über ein externes Relay senden.
- Das E-Mail-Gateway muss alle eingehenden E-Mails an die internen Mail-Server und aller andere (ausgehenden) Mails an das Gerät weiterleiten.
- Die Firewall erlaubt nur eingehende E-Mails, die sich an das Gerät richten.



Bei Firewalls, auf denen die Verwendung von NAT (Network Address Translation) konfiguriert ist und die eingehende E-Mails an die internen E-Mail-Server umleiten, müssen die öffentlichen MX-Einträge nicht neu konfiguriert werden. Sie leiten den Datenverkehr bereits an die Firewall und nicht an das eigentliche E-Mail-Gateway. In diesem Fall muss die Firewall neu konfiguriert werden, sodass eingehende Nachrichten an das Gerät geleitet werden.

Systemanforderungen

Stellen Sie mithilfe dieser Informationen sicher, dass Ihr Host-Computer die Systemanforderungen für die von Ihnen gewählte virtuelle VMware-Umgebung erfüllt.



Lesen Sie den VMware Knowledge Base-Artikel 1003661 unter http://www.vmware.com, um sich über die Mindestanforderungen an Ihr System für VMware ESX oder VMware ESXi 4.x zu informieren. Sie benötigen einen Computer mit einer 64-Bit-x86-CPU.

Darüber hinaus müssen Sie sicherstellen, dass die verwendete virtuelle Maschine die folgenden minimalen Systemanforderungen erfüllt:

Element	Spezifikation
Prozessor	Zwei virtuelle Prozessoren
Verfügbarer virtueller Speicher	2 GB
Freier Festplattenspeicher	80 GB



Wenn Sie planen, die McAfee Email Gateway Virtual Appliance im Modus "Transparente Bridge" zu installieren, benötigen Sie auf dem physischen VMware ESX-Host zwei externe Netzwerkschnittstellen, die mit verschiedenen Broadcast-Domänen verbunden sind. Aus Gründen der Leistungsoptimierung empfiehlt McAfee, diese beiden Schnittstellen nicht von anderen virtuellen Maschinen auf diesem physischen Host nutzen zu lassen. Wenn die beiden Schnittstellen einer Bridge mit derselben Broadcast-Domäne verbunden werden, entsteht in Ihrem Netzwerk eine STP-Schleife, die Netzwerkausfälle verursachen kann.

Beispiel-Installationsszenarien

In diesem Abschnitt enthalten Sie Informationen zur Installation der virtuellen Appliance in unterschiedlichen Server-Konfigurationen.

Ausführen der virtuellen Appliance als einzige virtuelle Maschine auf dem Host

Eine mögliche Ausbringung der virtuellen Appliance auf einem einzelnen Server in der von Ihnen gewählten virtuellen VMware-Umgebung.

VMware vSphere oder VMware vSphere Hypervisor sind dedizierte Server für die virtuelle Appliance. Deren Hardware-Spezifikation muss die minimalen Hardware-Anforderungen erfüllen, die in den *Richtlinien zu den McAfee Email Gateway-Leistungsdaten* dargelegt sind.



In diesem Beispiel wird davon ausgegangen, dass Sie die virtuelle Appliance im empfohlenen Modus "Expliziter Proxy" betreiben.

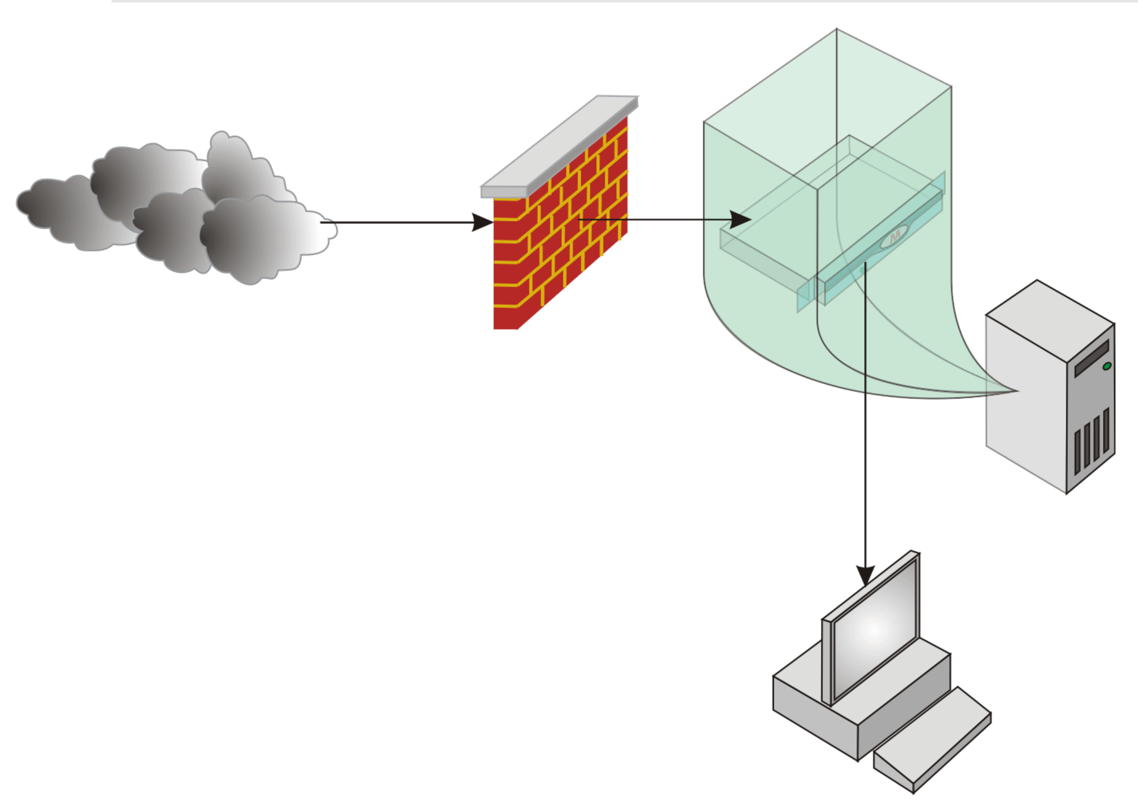


Abbildung 2-9 Ausbringung auf nur einem Server

Ausführen der virtuellen Appliance zusammen mit anderen virtuellen Maschinen

Eine mögliche Ausbringung von McAfee Email Gateway Virtual Appliance 7.0 in der von Ihnen gewählten virtuellen Umgebung neben anderen virtuellen Maschinen.

In diesem Beispiel ist ein VMware-Host für die virtuelle Appliance sowie auch für andere virtuelle Maschinen verantwortlich, die alle auf derselben Hardware ausgeführt werden. Auf der VMware-Website http://www.vmware.com finden Sie Informationen zum Aufbau eines

Ressourcen-Pools für die virtuelle Appliance. Dem Ressourcen-Pool müssen außerdem die Mindestanforderungen an CPU und Arbeitsspeicher zugewiesen sein, wie sie in den *Richtlinien zu den McAfee Email Gateway-Leistungsdaten* dargelegt sind.



In diesem Beispiel wird davon ausgegangen, dass Sie die virtuelle Appliance im empfohlenen Modus "Expliziter Proxy" betreiben.

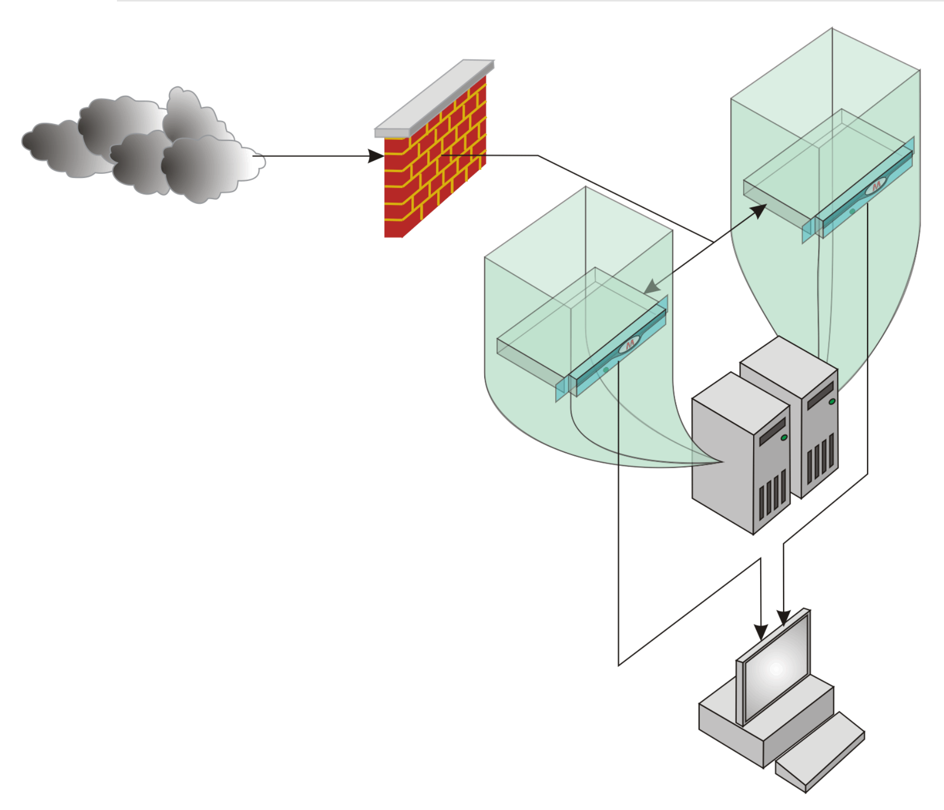


Abbildung 2-10 Ausbringung auf mehreren Servern

3 Installieren der McAfee Email Gateway Virtual Appliance

Diese Informationen helfen Ihnen dabei, die virtuelle Umgebung einzurichten und die McAfee Email Gateway Virtual Appliance 7.0 darauf zu installieren.

Inhalt

Übersicht über den Installationsvorgang der virtuellen Appliance

In diesem Abschnitt erhalten Sie einen kurzen Überblick über die Schritte, die zur Installation der virtuellen Appliance erforderlich sind.

McAfee empfiehlt, dass Sie die virtuelle Appliance in der folgenden Reihenfolge installieren:

1. Installieren Sie das gewünschte VMware-Produkt.
2. Laden Sie die Installationsdateien der virtuellen Appliance herunter.
3. Installieren Sie die virtuelle Appliance in der virtuellen Umgebung.
4. Führen Sie die Konfiguration mithilfe des grafischen Konfigurationsassistenten durch.
5. Melden Sie sich an der virtuellen Appliance an.

6. Testen Sie die Konfiguration.
7. Aktivieren Sie Protokolle.

Bewährte Vorgehensweisen für die Installation

Diese Informationen geben Ihnen einige wichtige Anhaltspunkte für die Installation auf VMware vSphere.



McAfee empfiehlt, dass Sie diese Informationen lesen und danach handeln, bevor Sie mit der Installation beginnen.

- Die virtuelle Appliance ist am einfachsten einzurichten und zu warten, wenn sie im standardmäßigen Betriebsmodus "Expliziter Proxy" betrieben wird.
- Machen Sie sich mit den Informationen zum Erstellen von Clustern und Ressourcen-Pools vertraut. Siehe die VMware-Website http://www.vmware.com.
- Verwenden Sie ein Storage Area Network (SAN) statt eines Network File System (NFS), um optimale Ergebnisse zu erzielen.
- Wenn Sie die virtuelle Appliance in einem der transparenten Modi betreiben:
  - Die Funktionen VMware Distributed Resource Scheduler (DRS) und High Availability (HA) könnnen zu Netzwerkunterbrechungen führen, wenn ein Failover stattfindet.
  - Stellen Sie sicher, dass die Netzwerkkarten der virtuellen Appliance nicht mit derselben Broadcast-Domäne verbunden sind und dass sich die IP-Adressen nicht in demselben Subnetz befinden, um Netzwerk-Loops zu vermeiden.
  - Stellen Sie sicher, dass jeder Netzwerkadapter auf der virtuellen Appliance mit einem anderen physischen Netzwerk auf dem Host-Computer verbunden ist.
  - Sie benötigen mindestens drei Netzwerkkarten im VMware-Host. Die virtuelle Appliance benötigt zwei Netzwerkkarten. VMware empfiehlt, eine dedizierte Netzwerkkarte für die Service-Konsole zu verwenden.

Vorgehensweise – Konvertieren einer VMtrial-Installation

Gehen Sie wie nachfolgend beschrieben vor, wenn Sie alle Konfigurationseinstellungen einer Installation von McAfee Email Gateway Appliance (VMtrial) auf McAfee Email Gateway Virtual Appliance 7.0 migrieren möchten.

Vorgehensweise

1. Wählen Sie in Ihrer VMtrial-Installation **System** | **Systemverwaltung** | **Konfigurationsverwaltung**.
2. Klicken Sie auf **Konfiguration sichern**, um die Konfigurationsdetails zu speichern.
3. Installieren Sie die Software für McAfee Email Gateway Virtual Appliance 7.0 in der gewünschten virtuellen Umgebung.
4. Melden Sie sich an, und öffnen Sie die Software für McAfee Email Gateway Virtual Appliance 7.0.
5. Wählen Sie **System** | **Systemverwaltung** | **Konfigurationsverwaltung**, und klicken Sie auf **Aus Datei wiederherstellen**.



Der Zugriff auf die Optionen zur Konfigurationswiederherstellung ist auch über **System** | **Setup-Assistent** möglich.

6 Gehen Sie zurück zur VMtrial-Konfigurationsdatei, die Sie wiederherstellen möchten, und klicken Sie auf **Öffnen**.

7 Wählen Sie die Teile der Datei aus, die Sie wiederherstellen möchten, und klicken Sie auf **OK**.

8 Überprüfen Sie, ob die Einstellungen erfolgreich importiert wurden, und übernehmen Sie die Änderungen.

Vorgehensweise – Herunterladen der Installations-Software

Gehen Sie wie nachfolgend beschrieben vor, um die aktuellste Version der McAfee Email Gateway-Software herunterzuladen.

Bevor Sie beginnen

- Lesen Sie das Installationshandbuch zu Ihrem -Produkt.
- Suchen Sie nach der McAfee-Grant-Nummer, die Sie beim Kauf von McAfee Email Gateway erhalten haben.

McAfee bietet die Software für die Installation in virtuellen Umgebungen als OVA-Datei an.

Vorgehensweise

1 Besuchen Sie die McAfee-Website http://www.mcafee.com. Halten Sie den Mauszeiger über Ihren Geschäftstyp, und klicken Sie auf **Downloads**.

2 Klicken Sie auf der Seite **Meine Produkte – Downloads** auf **Anmelden**.

3 Geben Sie die McAfee-Grant-Nummer ein, die Sie beim Kauf von McAfee Email Gateway erhalten haben, und klicken Sie auf **Senden**.

4 Wählen Sie aus der Produktliste **Email Gateway** aus.

5 Akzeptieren Sie die Lizenzbedingungen, wählen Sie die neueste Version, und laden Sie sie herunter.



McAfee empfiehlt, dass Sie die Versionsinformationen lesen, die Sie mit dem Software-Image erhalten, bevor Sie die Installation fortsetzen.

Vorgehensweise – Installation der Appliance auf VMware vSphere

Gehen Sie wie nachfolgend beschrieben vor, um McAfee Email Gateway Virtual Appliance 7.0 auf einem Host-Computer zu installieren, auf dem VMware vSphere 4 oder VMware vSphere Hypervisor (ESXi) 4.0 ausgeführt wird.

Bevor Sie beginnen

- Stellen Sie sicher, dass die VMware vSphere-Konfiguration die Arbeit mit dem gewählten Betriebsmodus ermöglicht.
- Laden Sie das Paket von McAfee Email Gateway Virtual Appliance 7.0 von der McAfee-Download-Seite herunter, und extrahieren Sie es in einen Speicherort, in dem es der VMware vSphere Client sehen kann.
- Installieren Sie eine lizenzierte Vollversion von VMware vSphere 4 oder VMware vSphere Hypervisor (ESXi) 4.

Wenn Sie das Produkt VMtrial verwendet haben, um die Software zu testen, können Sie Ihre VMtrial-Konfiguration speichern und im Anschuss an die Installation auf der virtuellen Appliance wiederherstellen.

Vorgehensweise

1. Starten Sie die VMware vSphere Client-Anwendung.
2. Melden Sie sich beim VMware vSphere-Server oder dem vCenter Server an.
3. Wählen Sie aus der Liste **Inventory** (Inventar) den Host oder Cluster, auf dem Sie die Software der virtuelle Appliance importieren möchten.
4. Klicken Sie auf **File | Deploy OVF Template | Deploy From File** (Datei | OVF-Vorlage bereitstellen | Aus Datei bereitstellen), klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem Speicherort, an dem Sie die .OVA-Datei heruntergeladen haben.
5. Wählen Sie die Datei **McAfee-MEG-7.0-<build_number>.VMbuy.ova**, und klicken Sie auf **Open** (Öffnen).
6. Klicken Sie zwei Mal auf **Next** (Weiter), und geben Sie optional einen neuen Namen ein.
7. Wählen Sie einen Ressourcen-Pool aus, sofern Sie einen konfiguriert haben.
8. Wählen Sie den Datenspeicher aus, und klicken Sie auf **Next** (Weiter).
9. Wählen Sie die virtuellen Netzwerke aus, mit denen die Netzwerkkarten der virtuellen Appliances verbunden werden.
10. Legen Sie die Größe der Festplatte für das Speichern von Daten fest, um den Speicherplatz zu erhöhen, der für isolierte, zurückgestellte und protokollierte Elemente reserviert wird.

    Für die Festplattengröße kann kein Wert definiert werden, der unterhalb der Standardgröße von 40 GB liegt.

11. Klicken Sie auf **Next** (Weiter), lesen Sie die Zusammenfassung, klicken Sie anschließend auf **Finish** (Fertig stellen), und warten Sie, bis der Importvorgang beendet ist.

Vorgehensweise – Verbessern der Systemleistung auf VMware vSphere

Mithilfe der folgenden Schritte können Sie möglicherweise die Systemleistung in VMware vSphere-Umgebungen steigern, indem Sie die Standardeinstellungen für Festplatten, Netzwerkadapter, Arbeitsspeicher und CPU ändern.

Vorgehensweise

1. So bearbeiten Sie die Festplatteneinstellungen:
   a. Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist.
   b. Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance in der Liste **Inventory** (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).

Im Dialogfeld **Virtual Machine Properties** (Eigenschaften der virtuellen Maschine) befinden sich drei Festplatten, die der virtuellen Appliance zur Verfügung stehen:

- **Hard disk 1** (Festplatte 1) enthält die Installationsdateien der virtuellen Appliance und darf weder entfernt noch verändert werden.
- **Hard disk 2** (Festplatte 2) ist die Hauptfestplatte, die von der virtuellen Appliance verwendet wird. Sie können deren Größe verändern, McAfee empfiehlt jedoch, sie nicht zu verkleinern.
- **Hard disk 3** (Festplatte 3) enthält den temporären Swap-Speicher der virtuellen Appliance.



Die Leistung kann möglicherweise erhöht werden, indem die zweite und die dritte Festplatte auf zwei getrennten Datenspeichern abgelegt werden.

2. So bearbeiten Sie die Einstellungen für Arbeitsspeicher und virtuelle CPU:
   - Prüfen Sie, ob die virtuelle Maschine ausgeschaltet ist.
   - Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance in der Liste "Inventory" (Inventar), und klicken Sie auf **Edit Settings** (Einstellungen bearbeiten).
   - Ändern Sie im Dialogfeld **Virtual Machine Properties** (Eigenschaften der virtuellen Maschine) die Einstellungen nach Bedarf.



McAfee empfiehlt, dass Sie die Einstellungen nicht auf weniger als die Standardeinstellungen oder die empfohlenen Systemanforderungen für die virtuelle Appliance herabsetzen.

Nach der Installation der Appliance kann die Größe der Festplatte nicht mehr verändert werden.

Konfiguration der virtuellen Appliance

Gehen Sie wie nachfolgend beschrieben vor, um die virtuelle Appliance zu konfigurieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihre virtuelle Umgebung installiert ist und ordnungsgemäß ausgeführt wird.

Vorgehensweise

1. Starten Sie die virtuelle Appliance. Die Installation beginnt automatisch.
2. Lesen Sie die Endbenutzer-Lizenzvereinbarung, um die Installation fortzusetzen, und klicken Sie dann auf **j**, um sie zu akzeptieren und mit der Installation zu beginnen.
3. Wählen Sie beim Installationsmenü **a** aus, um eine vollständige Installation auszuführen, und **j**, um fortzufahren.
4. Nachdem die Installation abgeschlossen ist, wird die virtuelle Appliance neu gestartet.
5. Wählen Sie im Eröffnungsfenster die Sprache aus, die Sie verwenden möchten.
6. Stimmen Sie den Bedingungen des Lizenzvertrags zu.
7. Konfigurieren Sie die virtuelle Appliance mithilfe des grafischen Konfigurationsassistenten.
8. Übernehmen Sie die Konfiguration auf die virtuelle Appliance. In Abhängigkeit von den eingegebenen Einstellungen wird möglicherweise ein Neustart durchgeführt. Sie können die

virtuelle Appliance auf mehr als einem VMware vSphere-, VMware vSphere Hypervisor- oder VMware Player-Server installieren. Gehen Sie dazu folgendermaßen vor:

a Führen Sie die Schritte in dieser Aufgabe auf einem anderen VMware vSphere-, VMware vSphere Hypervisor- oder VMware Player-Server aus.

b Kehren Sie zur Benutzeroberfläche der zuvor installierten virtuelle Appliance zurück.

c Gehen Sie zu **System** | **Systemverwaltung** | **Konfigurations-Push**, um die Konfigurationsdetails an die zweite virtuelle Appliance zu senden.

Verwenden der Konfigurationskonsole

Erfahren Sie, wie Sie Ihr McAfee® Email GatewayMcAfee Email Gateway mithilfe der Konfigurationskonsole einrichten.

Sie können Ihr McAfee® Email Gateway jetzt entweder von der Konfigurationskonsole aus oder innerhalb der Benutzeroberfläche mit dem Setup-Assistenten konfigurieren.

Die Konfigurationskonsole wird am Ende der Startsequenz automatisch gestartet, entweder nachdem:

- ein unkonfiguriertes E-Mail-Gateway gestartet wurde
- oder nachdem ein E-Mail-Gateway auf die Werkseinstellungen zurückgesetzt wurde.

Wird die Konfigurationskonsole gestartet, bietet Sie Ihnen die Möglichkeit, Ihr E-Mail-Gateway von der E-Mail-Konsole aus in Ihrer bevorzugten Sprache zu konfigurieren, bzw. liefert Anweisungen dafür, wie Sie von einem anderen Computer im selben Klasse-C-Subnetz aus eine Verbindung mit dem Setup-Assistenten innerhalb der Benutzeroberfläche herstellen können. Beide Methoden bieten Ihnen dieselben Optionen für die Konfiguration Ihres E-Mail-Gateways.



Von der Konfigurationskonsole aus können Sie eine neue Installation der Appliance-Software konfigurieren. Wenn Sie jedoch für die Konfiguration Ihrer Appliance eine zuvor gespeicherte Konfigurationsdatei verwenden möchten, müssen Sie sich bei der Benutzeroberfläche der Appliance anmelden und den Setup-Assistenten ausführen (**System** | **Setup-Assistent**).

Ebenso wird mit dieser Softwareversion für folgende Parameter die automatische Konfiguration mithilfe von DHCP eingeführt:

- Host-Name
- Domänenname
- Standard-Gateway
- DNS-Server
- Geleaste IP-Adresse
- NTP-Server

Begrüßung

Auf dieser Seite können Sie den gewünschten Installationstyp auswählen.

Dies ist die erste Seite des Setup-Assistenten. Auf dieser Seite können Sie den gewünschten Installationstyp auswählen.

- **Standardeinrichtung** (Standardeinstellung) – Verwenden Sie diese Option, um das Gerät im Modus "Transparente Bridge" einzurichten und für den Schutz Ihres Netzwerks zu konfigurieren. Das SMTP-Protokoll ist standardmäßig aktiviert. Sie können wählen, ob POP3-Verkehr gescannt werden soll.

  Mit der Wahl der **Standardeinrichtung** wird für das Gerät der Modus "Transparente Bridge" erzwungen.

- **Benutzerdefinierte Einrichtung** – Verwenden Sie diese Option, um den Betriebsmodus für Ihr Gerät auszuwählen. Sie können auswählen, dass der E-Mail-Verkehr über die Protokolle SMTP und POP3 geschützt wird. Verwenden Sie diese Art der Einrichtung, um IPv6 zu konfigurieren und sonstige Änderungen an der Standardkonfiguration vorzunehmen.
- **Aus Datei wiederherstellen** (auf der Konfigurationskonsole nicht verfügbar) – Verwenden Sie diese Option, um Ihr Gerät basierend auf einer zuvor gespeicherten Konfiguration einzurichten. Nach dem Importieren der Datei können Sie die importierten Einstellungen überprüfen, bevor Sie den Assistenten abschließen. Wenn die Datei aus einer früheren McAfee Email and Web Security Appliance stammt, sind einige Details nicht verfügbar.
- **Einrichten der Verwaltung durch ePolicy Orchestrator** – Verwenden Sie diese Option, um Ihr Gerät so zu konfigurieren, dass es von Ihrem ePolicy Orchestrator® -Server (McAfee ePO™) aus verwaltet werden kann. Es wird nur ein Minimum an Informationen benötigt, da das Gerät die meisten Konfigurationsdaten vom ePolicy Orchestrator-Server enthält.
- **Setup im Modus "Nur Verschlüsselung"** – Verwenden Sie diese Option, um die Appliance als eigenständigen Verschlüsselungs-Server einzurichten.

Die Appliance wird in einem der folgenden Modi betrieben: "Transparente Bridge", "Transparenter Router" oder "Expliziter Proxy". Der Modus wirkt sich auf die Integration der Appliance im Netzwerk aus und darauf, wie die Appliance den Datenverkehr verarbeitet. Sie müssen den Modus nur ändern, wenn das Netzwerk neu strukturiert wird.

Durchführen der Standardeinrichtung

In diesem Abschnitt erfahren Sie, welchen Zweck die Standardeinrichtung hat.

Die **Standardeinrichtung** ermöglicht Ihnen die schnelle Einrichtung Ihres McAfee Email Gateways unter Verwendung der gängigsten Optionen. Verwenden Sie diese Option, um das Gerät im Modus "Transparente Bridge" einzurichten und für den Schutz Ihres Netzwerks zu konfigurieren. Das SMTP-Protokoll ist standardmäßig aktiviert. Sie können wählen, ob POP3-Verkehr gescannt werden soll.



Mit der Wahl der **Standardeinrichtung** wird für das Gerät der Modus "Transparente Bridge" erzwungen.

Bei der **Standardeinrichtung** enthält der Assistent die folgenden Seiten:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Zusammenfassung**

Seite "E-Mail-Konfiguration" (Standardeinrichtung)

Hier werden die auf dieser Seite verfügbaren Optionen beschrieben.

Option	Beschreibung
Schutz vor potenziell unerwünschten Programme aktivieren	Klicken Sie hier, um den Schutz vor potenziell unerwünschten Programmen zu aktivieren. Lesen Sie die Hinweise von McAfee zu den Auswirkungen, die das Aktivieren dieses Schutzes haben kann.
McAfee Global Threat Intelligence-Feedback aktivieren	Wählen Sie diese Option aus, um McAfee Global Threat-Feedback zu aktivieren. Klicken Sie auf **Was ist das?**, um Informationen darüber zu erhalten, wie das Feedback genutzt wird, und die McAfee-Datenschutzrichtlinien anzuzeigen.
Lokale Relay-Domäne	Geben Sie sowohl die IP-Adresse als auch die Netzmaske für Ihre lokale Relay-Domäne ein.

Seite "Grundlegende Einstellungen" (Standardeinrichtung)

Verwenden Sie diese Seite im Assistenten für die Standardeinrichtung, um grundlegende Einstellungen für die Appliance im Modus "Transparente Bridge" anzugeben.

Option	Beschreibung
Gerätename	Gibt einen Namen an, z. B. Appliance1.
Domänenname	Gibt einen Domänennamen an, z. B. domaene1.com.
IP address	Gibt eine IP-Adresse an, z. B. 198.168.200.10. Der vollqualifizierte Domänenname (**Gerätename**. **Domänenname**) muss in diese IP-Adresse aufgelöst werden, wenn der (hier angegebene) DNS-Server aufgerufen wird. Wir empfehlen, dass diese IP-Adresse bei umgekehrten Suchen in den vollqualifizierten Domänennamen aufgelöst wird.
Subnetz	Gibt eine Subnetzadresse an, z. B. 255.255.255.0.
Gateway-Adresse	Gibt eine IP-Adresse an, z. B. 198.168.10.1. Hierbei handelt es sich meist um einen Router oder eine Firewall. Sie können später testen, ob die Appliance mit diesem Gerät kommunizieren kann.
DNS-Server-IP	Gibt die Adresse eines Domänennamenservers an, den die Appliance verwendet, um Website-Adressen in IP-Adressen umzuwandeln. Dabei kann es sich um einen Active Directory- oder einen DNS-Server handeln. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Modus	Gibt den Modus an ("Transparente Bridge", "Transparenter Router" oder "Expliziter Proxy").
Benutzer-ID	Beim Benutzer "scmadmin" handelt es sich um den Superadministrator. Dieses Konto kann weder geändert oder deaktiviert noch gelöscht werden. Nach der Installation können Sie jedoch weitere Anmeldekonten hinzufügen.
Aktuelles Kennwort/ Neues Kennwort	Das ursprüngliche Standardkennwort lautet `password`. Geben Sie das neue Kennwort an. Ändern Sie das Kennwort baldmöglichst, damit Ihre Appliance geschützt bleibt. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen.
Zeitzone der Appliance	Gibt die Zeitzone der Appliance an. Wenn in Ihrer Region Sommer- und Winterzeit gelten, müssen Sie die Zeitzone zweimal im Jahr ändern. Die Zonen sind von West nach Ost organisiert und decken den pazifischen Raum, Amerika, Europa, Asien, Afrika, Indien, Japan und Australien ab.
Appliance-Zeit (UTC)	Gibt das Datum und die UTC-Zeit für die Appliance an. Um das Datum festzulegen, klicken Sie auf das Kalendersymbol. Sie können die UTC-Zeit von Websites ablesen, wie http://www.worldtimeserver.com.
Jetzt einstellen	Wenn Sie hierauf klicken, werden das Datum und die UTC-Zeit, die Sie in dieser Zeile ausgewählt haben, angewendet.
Client-Zeit	Zeigt die Zeit entsprechend dem Client-Computer an, von dem aus Ihr Browser derzeit mit der Appliance verbunden ist.
Appliance mit Client synchronisieren	Bei Auswahl übernimmt die Zeit unter **Appliance-Zeit (UTC)** sofort den Wert aus **Client-Zeit**. Sie können dieses Kontrollkästchen als Alternative verwenden, um manuell die **Appliance-Zeit (UTC)** einzustellen. Die Appliance errechnet die UTC-Zeit basierend auf der Zeitzone, die sie im Client-Browser findet. Stellen Sie sicher, dass der Client-Computer Sommer- und Winterzeit berücksichtigt. Um die Einstellung in Microsoft Windows zu finden, klicken Sie mit der rechten Maustaste in die untere rechte Ecke des Bildschirms.
NTP-Serveradresse	Um das Network Time Protocol (NTP) zu verwenden, geben Sie die Serveradresse an. Alternativ dazu können Sie NTP später konfigurieren.

Seite "Zusammenfassung" (Standardeinrichtung)

Im Assistenten für die Standardeinrichtung können Sie auf dieser Seite eine Zusammenfassung der Einstellungen anzeigen, die Sie für Netzwerkverbindungen und das Scannen des Netzwerkverkehrs vorgenommen haben.

Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen und die Appliance ist als transparente Bridge konfiguriert.

Verwenden Sie die hier angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: https://192.168.200.10.



Die Adresse beginnt mit https und nicht mit http.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **admin** und das Kennwort ein, das Sie auf der Seite **Grundlegende Einstellungen** angegeben haben.

Tabelle 3-1 Grundlegende Einstellungen

Option	Beschreibung
	Der Wert entspricht bewährten Praktiken.
	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

Durchführen der benutzerdefinierten Einrichtung

In diesem Abschnitt erfahren Sie, welchen Zweck die benutzerdefinierte Einrichtung hat.

Die **Benutzerdefinierte Einrichtung** ermöglicht Ihnen eine größere Kontrolle über die Optionen, die Sie auswählen können, darunter den Betriebsmodus des Geräts. Sie können auswählen, dass der E-Mail-Verkehr über die Protokolle SMTP und POP3 geschützt wird. Verwenden Sie diese Konfigurationsoption, um IPv6 zu konfigurieren und sonstige Änderungen an der Standardkonfiguration vorzunehmen.

Bei der **Benutzerdefinierten Einrichtung** enthält der Assistent die folgenden Seiten:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **DNS und Routing**
- **Zeiteinstellungen**
- **Kennwort**
- **Zusammenfassung**

Seite "Grundlegende Einstellungen" (Benutzerdefinierte Einrichtung)

Im Assistenten "Benutzerdefinierte Einrichtung" geben Sie auf dieser Seite die grundlegenden Einstellungen der Appliance an.

Die Appliance versucht, Ihnen einige Informationen zur Verfügung zu stellen, und zeigt die Informationen gelb markiert an. Um diese Informationen zu ändern, klicken Sie, und geben Sie sie erneut ein.

Option	Beschreibung
Cluster-Modus	Definiert die Optionen, die auf der Seite **Cluster-Verwaltung** des Setup-Assistenten erscheinen. • **Aus** – Dies ist eine Standard-Appliance. • **Cluster-Scanner** – Die Appliance empfängt ihre Scan-Arbeit von einer Master-Appliance. • **Cluster-Master** – Die Appliance steuert die Scan-Arbeit verschiedener anderer Appliances. • **Cluster-Failover** – Falls der Master ausfällt, steuert diese Appliance stattdessen die Scan-Arbeit.
Gerätename	Gibt einen Namen an, z. B. Appliance1.
Domänenname	Gibt einen Domänennamen an, z. B. domaene1.com.
Standard-Gateway	Gibt eine IPv4-Adresse an, z. B. 198.168.10.1. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Nächster Router	Gibt eine IPv6-Adresse an, z. B. FD4A:A1B2:C3D4::1.
Netzwerkschnittstelle	Wird verfügbar, wenn Sie das Feld **Nächster Router** für IPv6 festlegen.

Seite "Netzwerkeinstellungen"

Verwenden Sie diese Optionen, um die IP-Adresse und die Netzwerkgeschwindigkeiten für die Appliance anzuzeigen und zu konfigurieren. Sie können IPv4- und IPv6-Adressen verwenden, entweder separat oder zusammen.

Vergeben Sie neue IP-Adressen für die Appliance und deaktivieren Sie die standardmäßigen IP-Adressen, um doppelte IP-Adressen im Netzwerk zu vermeiden und um Hacker abzuhalten. Die IP-Adressen müssen eindeutig und für Ihr Netzwerk geeignet sein. Geben Sie so viele IP-Adressen wie erforderlich an.

Option	Beschreibung
<mode>	Der Betriebsmodus, den Sie während der Installation oder im Setup-Assistenten festlegen.
Netzwerkschnittstelle 1	Wird erweitert und zeigt die IP-Adresse und die Netzmaske für die Netzwerkschnittstelle 1, den Autonegotiation-Status und die MTU-Größe an.
Netzwerkschnittstelle 2	Wird erweitert und zeigt die IP-Adresse und die Netzmaske für die Netzwerkschnittstelle 2, den Autonegotiation-Status und die MTU-Größe an.
Netzwerkeinstellungen ändern	Klicken Sie hier, um den Netzwerkschnittstellen-Assistenten zu öffnen, um die IP-Adresse und die Adaptereinstellungen für NIC 1 und NIC 2 anzugeben und den ausgewählten Betriebsmodus zu ändern.
Netzwerkschnittstellenlayout anzeigen	Klicken Sie hier, um das <?> zu sehen, das mit LAN1, LAN2 und der Out-of-Band-Schnittstelle verknüpft ist.

Netzwerkschnittstellen-Assistent

Verwenden Sie den Netzwerkschnittstellen-Assistenten, um den ausgewählten Betriebsmodus zu ändern und die IP-Adresse und die Adaptereinstellungen für NIC 1 und NIC 2 anzugeben.

Die Optionen, die im Netzwerkschnittstellen-Assistenten angezeigt werden, hängen vom Betriebsmodus ab. Auf der ersten Seite des Assistenten können Sie den Betriebsmodus der Appliance ändern. Sie können die Einstellungen durch Klicken auf **Netzwerkeinstellungen ändern** ändern, wodurch ein Assistent gestartet wird. Klicken Sie auf **Weiter**, um jeweils zur nächsten Assistentenseite zu gelangen.

Im Modus **Expliziter Proxy** senden einige Netzwerkgeräte Datenverkehr an die Appliances. Die Appliance fungiert dann als **Proxy** und verarbeitet den Datenverkehr für die Geräte.

Im Modus **Transparenter Router** oder **Transparente Bridge** wissen andere Netzwerkgeräte wie E-Mail-Server nicht, dass die Appliance die E-Mail vor dem Weiterleiten abgefangen und gescannt hat. Der Vorgang auf der Appliance ist für andere Geräte transparent, also unsichtbar.



Wenn Sie eine eigenständige Appliance verwenden, die im Modus "Transparente Bridge" betrieben wird, haben Sie die Möglichkeit, für den Fall, dass bei der Appliance ein Fehler auftritt, ein Bypass-Gerät hinzuzufügen.

Wenn die Appliance im Modus "Transparente Bridge" betrieben wird und Sie in Ihrem Netzwerk das Spanning Tree-Protokoll (STP) ausführen, müssen Sie sicherstellen, dass die Appliance gemäß den STP-Regeln konfiguriert ist. Außerdem können Sie im Modus "Transparente Bridge" ein Umleitungsgerät einrichten.

Netzwerkschnittstellen-Assistent – Modus "Expliziter Proxy"

Verwenden Sie den Netzwerkschnittstellen-Assistenten, um den ausgewählten Betriebsmodus zu ändern und die IP-Adresse und die Adaptereinstellungen für NIC 1 und NIC 2 anzugeben.

Diese Version des Netzwerkschnittstellen-Assistenten wird verfügbar, wenn Sie den Modus "Expliziter Proxy" auswählen.



Legen Sie die Details für "Netzwerkschnittstelle 1" fest, und klicken Sie anschließend bei Bedarf auf die Schaltfläche **Weiter**, um Details für die "Netzwerkschnittstelle 2" festzulegen.

Seite "Netzwerkschnittstelle 1" oder "Netzwerkschnittstelle 2"

Option	Beschreibung
IP-Adresse	Gibt Netzwerkadressen an, die es der Appliance ermöglichen, mit Ihrem Netzwerk zu kommunizieren. Sie können mehrere IP-Adressen für die Netzwerkanschlüsse der Appliance angeben. Bei der ersten IP-Adresse in der Liste handelt es sich um die *primäre* Adresse. Bei den nachfolgenden IP-Adressen handelt es sich um *Aliasse*. Sie müssen mindestens über jeweils eine IP-Adresse in "Netzwerkschnittstelle 1" und "Netzwerkschnittstelle 2" verfügen. Sie können jedoch die Auswahl der Option **Aktiviert** neben allen IP-Adressen aufheben, die Sie nicht überwachen möchten.
Netzwerkmaske	Gibt die Netzwerkmaske an. In IPv4 können Sie ein Format wie `255.255.255.0` oder eine CIDR-Notation wie `24` verwenden. In IPv6 müssen Sie die Präfixlänge verwenden, z. B. `64`.
Aktiviert	Wenn diese Option ausgewählt ist, akzeptiert die Appliance Verbindungen auf der IP-Adresse.
Virtuell	Wenn diese Option ausgewählt ist, behandelt die Appliance diese IP-Adresse als virtuelle Adresse. Diese Option wird nur in Cluster-Konfigurationen oder auf einem McAfee Content Security Blade Server angezeigt.

Option	Beschreibung
Neue Adresse/ Ausgewählte Adressen löschen	Fügen Sie eine neue Adresse hinzu, oder entfernen Sie eine ausgewählte IP-Adresse.
Adapteroptionen für NIC 1 oder **Adapteroptionen für NIC 2**	Erweitern Sie den entsprechenden Eintrag, um die folgenden Optionen einzurichten: • **MTU-Größe** – Gibt die MTU-Größe (Maximum Transmission Unit) an. Bei MTU handelt es sich um die maximale Größe (in Byte) einer einzelnen Dateneinheit (z. B. ein Ethernet-Rahmen), die über die Verbindung gesendet werden kann. Der Standardwert ist 1.500 Byte. • **Autonegotiations-Status** – Entweder: • **Ein** – Ermöglicht, dass die Appliance die Geschwindigkeit und den Duplex-Status für die Kommunikation mit anderen Netzwerkgeräten aushandelt. • **Aus** – Ermöglicht es dem Benutzer, die Geschwindigkeit und den Duplex-Status auszuwählen. • **Verbindungsgeschwindigkeit** – Bietet einen Bereich mit Verbindungsgeschwindigkeiten. Der Standardwert lautet 100 MB. Der Maximalwert liegt bei 1 GB für Glasfasersysteme. • **Duplex-Status** – Bietet Duplex-Status. Beim Standardwert handelt es sich um "Vollduplex". • **Automatische Konfiguration von IPv6 aktivieren** – Wählen Sie diese Option aus, um der Appliance die automatische Konfiguration ihrer IPv6-Adressen und IPv6-Next-Hop-Standardrouter durch den Empfang von vom IPv6-Router gesendeten Nachrichten zum Router Advertisement (Router-Ankündigung) zu ermöglichen. Diese Option ist standardmäßig nicht verfügbar, wenn die Appliance im Modus "Transparenter Router" betrieben wird, einer Cluster-Konfiguration angehört oder als Teil einer Blade-Server-Installation betrieben wird.

Netzwerkschnittstellen-Assistent – Modus "Transparenter Router"

Verwenden Sie den Netzwerkschnittstellen-Assistenten, um den ausgewählten Betriebsmodus zu ändern und die IP-Adresse und die Adaptereinstellungen für NIC 1 und NIC 2 anzugeben.

Seite "Netzwerkschnittstelle 1" oder "Netzwerkschnittstelle 2"

Option	Beschreibung
IP-Adresse	Gibt Netzwerkadressen an, die es der Appliance ermöglichen, mit Ihrem Netzwerk zu kommunizieren. Sie können mehrere IP-Adressen für die Anschlüsse der Appliance angeben. Bei der ersten IP-Adresse in der Liste handelt es sich um die primäre Adresse. Bei den nachfolgenden IP-Adressen handelt es sich um *Aliasse*.
Netzwerkmaske	Gibt die Netzwerkmaske an, z. B.: 255.255.255.0. In IPv4 können Sie ein Format wie `255.255.255.0` oder eine CIDR-Notation wie `24` verwenden. In IPv6 müssen Sie die Präfixlänge verwenden, z. B. `64`.
Aktiviert	Wenn diese Option ausgewählt ist, akzeptiert die Appliance Verbindungen auf dieser IP-Adresse.
Virtuell	Wenn diese Option ausgewählt ist, behandelt die Appliance diese IP-Adresse als virtuelle Adresse. Diese Option wird nur in Cluster-Konfigurationen oder auf einem McAfee Content Security Blade Server angezeigt.

Option	Beschreibung
Neue Adresse/ Ausgewählte Adressen löschen	Fügen Sie eine neue Adresse hinzu, oder entfernen Sie eine ausgewählte IP-Adresse.
Adapteroptionen für NIC 1 oder **Adapteroptionen für NIC 2**	Erweitern Sie den entsprechenden Eintrag, um die folgenden Optionen einzurichten: • **MTU-Größe** – Gibt die MTU-Größe (Maximum Transmission Unit) an. Bei der MTU handelt es sich um die maximale Größe (in Byte) einer einzelnen Dateneinheit (z. B. ein Ethernet-Rahmen), die über die Verbindung gesendet werden kann. Der Standardwert ist 1.500 Byte. • **Autonegotiations-Status** – Entweder: • **Ein** – Ermöglicht, dass die Appliance die Geschwindigkeit und den Duplex-Status für die Kommunikation mit anderen Netzwerkgeräten aushandelt. • **Aus** – Ermöglicht es dem Benutzer, die Geschwindigkeit und den Duplex-Status auszuwählen. • **Verbindungsgeschwindigkeit** – Bietet einen Bereich mit Verbindungsgeschwindigkeiten. Der Standardwert lautet 100 MB. Der Maximalwert liegt bei 1 GB für Glasfasersysteme. • **Duplex-Status** – Bietet Duplex-Status. Beim Standardwert handelt es sich um "Vollduplex". • **Automatische Konfiguration von IPv6 aktivieren** – Wählen Sie diese Option aus, um der Appliance die automatische Konfiguration ihrer IPv6-Adressen und IPv6-Next-Hop-Standardrouter durch den Empfang von vom IPv6-Router gesendeten Nachrichten zur Router-Bekanntgabe zu ermöglichen. Diese Option ist standardmäßig nicht verfügbar, wenn die Appliance im Modus "Transparenter Router" betrieben wird, einer Cluster-Konfiguration angehört oder als Teil einer Blade-Server-Installation betrieben wird. • **Senden von IPv6-Router-Advertisements auf dieser Schnittstelle aktivieren** – Wenn diese Option aktiviert ist, können IPv6-Router-Advertisements an Computer in einem Subnetz gesendet werden, die eine Reaktion des Routers benötigen, damit eine automatische Konfiguration abgeschlossen werden kann.

Netzwerkschnittstellen-Assistent – Modus "Transparente Bridge"

Verwenden Sie den Netzwerkschnittstellen-Assistenten, um den ausgewählten Betriebsmodus zu ändern und die IP-Adresse und die Adaptereinstellungen für NIC 1 und NIC 2 anzugeben.



Legen Sie die Details für die Ethernet-Bridge fest, und klicken Sie anschließend auf die Schaltfläche **Weiter**, um ggf. Details für das Spanning Tree-Protokoll und das Bypass-Gerät festzulegen.

Optionsbeschreibungen – Seite "Ethernet-Bridge"

Option	Beschreibung
Alle auswählen	Klicken Sie hier, um alle IP-Adressen auszuwählen.
IP-Adresse	Gibt Netzwerkadressen an, die es der Appliance ermöglichen, mit Ihrem Netzwerk zu kommunizieren. Sie können mehrere IP-Adressen für die Anschlüsse der Appliance angeben. Die IP-Adressen für beide Anschlüsse werden in einer Liste kombiniert. Bei der ersten IP-Adresse in der Liste handelt es sich um die primäre Adresse. Bei den nachfolgenden IP-Adressen handelt es sich um *Aliasse*. Verwenden Sie die **Verschieben**-Links, um die Adressen nach Bedarf neu zu positionieren.

Option	Beschreibung
Netzwerkmaske	Gibt die Netzwerkmaske an, z. B.: 255.255.255.0. In IPv4 können Sie ein Format wie `255.255.255.0` oder eine CIDR-Notation wie `24` verwenden. In IPv6 müssen Sie die Präfixlänge verwenden, z. B. `64`.
Aktiviert	Wenn diese Option ausgewählt ist, akzeptiert die Appliance Verbindungen auf dieser IP-Adresse.
Neue Adresse/ Ausgewählte Adressen löschen	Fügen Sie eine neue Adresse hinzu, oder entfernen Sie eine ausgewählte IP-Adresse.
NIC-Adapteroptionen	Erweitern Sie den entsprechenden Eintrag, um die folgenden Optionen einzurichten: • **MTU-Größe** – Gibt die MTU-Größe (Maximum Transmission Unit) an. Bei MTU handelt es sich um die maximale Größe (in Byte) einer einzelnen Dateneinheit (z. B. ein Ethernet-Rahmen), die über die Verbindung gesendet werden kann. Der Standardwert ist 1.500 Byte. • **Autonegotiations-Status** – Entweder: • **Ein** – Ermöglicht, dass die Appliance die Geschwindigkeit und den Duplex-Status für die Kommunikation mit anderen Netzwerkgeräten aushandelt. • **Aus** – Ermöglicht es dem Benutzer, die Geschwindigkeit und den Duplex-Status auszuwählen. • **Verbindungsgeschwindigkeit** – Bietet einen Bereich mit Verbindungsgeschwindigkeiten. Der Standardwert lautet 100 MB. Der Maximalwert liegt bei 1 GB für Glasfasersysteme. • **Duplex-Status** – Bietet Duplex-Status. Beim Standardwert handelt es sich um "Vollduplex". • **Automatische Konfiguration von IPv6 aktivieren** – Wählen Sie diese Option aus, um der Appliance die automatische Konfiguration ihrer IPv6-Adressen und IPv6-Next-Hop-Standardrouter durch den Empfang von vom IPv6-Router gesendeten Nachrichten zum Router Advertisement (Router-Ankündigung) zu ermöglichen. Diese Option ist standardmäßig nicht verfügbar, wenn die Appliance im Modus "Transparenter Router" betrieben wird, einer Cluster-Konfiguration angehört oder als Teil einer Blade-Server-Installation betrieben wird.

Optionsbeschreibungen – Seite "Spanning Tree-Protokolleinstellungen"

Option	Beschreibung
STP aktivieren	STP ist standardmäßig aktiviert.
Bridge-Priorität	Legt die Priorität für die STP-Bridge fest. Niedrigere Zahlen haben eine höhere Priorität. Sie können eine Höchstzahl von 65535 festlegen.
Erweiterte Parameter	Erweitern Sie den entsprechenden Eintrag, um die folgenden Optionen einzurichten. Ändern Sie die Einstellungen nur, wenn Sie sich über die möglichen Auswirkungen im Klaren sind oder einen Experten befragt haben. • **Weiterleitungsverzögerung** • **Intervall für Garbage-Collection (Sekunden)** • **Intervall für Hello (Sekunden)** • **Alterungszeit (Sekunden)** • **Maximales Alter (Sekunden)**

Optionsbeschreibungen – Einstellungen für Bypass-Gerät

Option	Beschreibung
	Das Bypass-Gerät erbt die Einstellungen von den Angaben unter **NIC-Adapteroptionen**. .
Bypass-Gerät auswählen	Wählen Sie aus zwei unterstützten Geräten aus.
Watchdog-Zeitüberschreitung (Sekunden)	Für das Bypass-Gerät: Die Zeit in Sekunden, die verstreichen kann, bevor das System die Appliance umgeht.
Heartbeat-Intervall (Sekunden)	Standardmäßig ist die Überwachung des Heartbeats eingestellt.
Erweiterte Parameter	Diese Option wird aktiv, wenn Sie ein Bypass-Gerät auswählen. • **Modus** – Wählen Sie, ob nur der Heartbeat oder der Heartbeat und die Link-Aktivität überwacht werden sollen. • **Zeitüberschreitung für Link-Aktivität (Sekunden)** – Wird aktiv, wenn Sie **Heartbeat und Link-Aktivitäten überwachen** unter **Modus** auswählen. • **Buzzer aktivieren** – Ist standardmäßig aktiviert. Wenn das Bypass-Gerät nicht das Heartbeat-Signal für die konfigurierte **Watchdog-Zeitüberschreitung** erkennt, ertönt der Buzzer.

Seite "Cluster-Verwaltung"

Auf dieser Seite können Sie die Lastverteilung im Cluster konfigurieren.



Abhängig davon, welchen Cluster-Modus Sie auf der Seite **Grundlegende Einstellungen** ausgewählt haben, ändern sich die auf der Seite **Cluster-Verwaltung** angezeigten Optionen.

Konfiguration der Cluster-Verwaltung (Standard-Appliance)

Nicht verwenden. Die Cluster-Verwaltung ist deaktiviert.

Cluster-Verwaltung (Cluster-Scanner)

Option	Beschreibung
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.

Cluster-Verwaltung (Cluster-Master)



Im Modus "Expliziter Proxy" oder "Transparenter Router" können Sie das Failover zwischen zwei Appliances in einem Cluster aktivieren, indem Sie dieser Appliance eine virtuelle IP-Adresse zuweisen und eine andere Appliance als Cluster-Failover-Appliance mit derselben virtuellen Adresse konfigurieren. Im Modus "Transparente Bridge" erreichen Sie dies, indem Sie eine hohe STP-Priorität für diese Appliance einrichten und eine andere Appliance als Cluster-Failover-Appliance mit einer geringeren STP-Priorität konfigurieren.

Option	Beschreibung
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. Wenn Sie in einem Appliance-Cluster nur über eine Master- und eine Failover-Appliance verfügen, die beide für das Scannen des Datenverkehrs konfiguriert sind, sendet die Master-Appliance die meisten Verbindungen zum Scannen an die Failover-Appliance.

Optionsbeschreibungen – Erweiterte Einstellungen für Scan-Geräte

Verwenden Sie diesen Bereich für die detaillierte Kontrolle der verbundenen Scan-Geräte. Sie können die Geräte auch für die gemeinsame Nutzung von Festplattenspeicher zur Speicherung von Secure Web Mail-Nachrichten konfigurieren. Geräte in einem Cluster werden über ihre MAC-Adressen (Media Access Control) identifiziert. Wenn Sie der Tabelle eine MAC-Adresse hinzufügen, können Sie diese deaktivieren, sodass keine Scan-Anfragen an das Gerät gesendet werden. Außerdem können Sie Festplattenspeicher gemeinsam nutzen.

Option	Beschreibung
MAC-Adresse	Gibt die MAC-Adresse (Media Access Control) des Geräts mit 12 Hexadezimalstellen im folgenden Format an: A1:B2:C3:D4:E5:F6.
Deaktiviert	Wählen Sie diese Option, wenn Sie dieses Gerät aus der Gruppe der Scan-Geräte entfernen möchten.
MAC-Adresse hinzufügen	Klicken Sie auf diese Schaltfläche, wenn Sie die MAC-Adresse eines neuen Geräts hinzufügen möchten.
MAC-Adressen verwalten	Öffnet das Dialogfeld "MAC-Adressen", in dem Sie die Liste der verfügbaren MAC-Adressen verwalten können.



Obwohl Sie dieser Tabelle die MAC-Adressen der Management- und Failover-Geräte hinzufügen können, können diese nicht deaktiviert werden, da sie immer Festplattenspeicher für Secure Web Mail-Nachrichten bereitstellen.

Cluster-Verwaltung (Cluster-Failover)

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an. Bietet eine Liste aller einer Appliance zugewiesenen Subnetze.
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. Wenn Sie in einem Appliance-Cluster nur über eine Master- und eine Failover-Appliance verfügen, die beide für das Scannen des Datenverkehrs konfiguriert sind, sendet die Master-Appliance die meisten Verbindungen zum Scannen an die Failover-Appliance.

Seite "DNS und Routing"

Verwenden Sie diese Seite, um die Verwendung von DNS und Routen durch die Appliance zu konfigurieren.

DNS-Server (Domain Name System) übersetzen die Namen von Netzwerkgeräten in IP-Adressen (und umgekehrt), d. h., sie ordnen die Namen und Adressen einander zu. Die Appliance sendet in der hier aufgeführten Reihenfolge Anfragen an DNS-Server.

DNS-Server-Adressen

Option	Beschreibung
Server-Adresse	Zeigt die IP-Adressen der DNS-Server an. Beim ersten Server in der Liste muss es sich um den schnellsten bzw. zuverlässigsten Server handeln. Falls der erste Server die Anforderung nicht auflösen kann, nimmt die Appliance Kontakt mit dem zweiten Server auf. Falls keiner der Server in der Liste die Anforderung auflösen kann, leitet die Appliance die Anforderung an die DNS-Root-Namenserver im Internet weiter. Geben Sie die IP-Adresse eines lokalen Geräts mit Namensauflösungsfunktion an, wenn DNS-Suchen (in der Regel auf Port 53) von der Firewall verhindert werden.
Neuer Server/ Ausgewählte Server löschen	Fügt einen neuen Server zur Liste hinzu oder entfernt einen Server, beispielsweise, wenn Sie einen Server aufgrund von Netzwerkänderungen außer Betrieb setzen müssen.
Nur Anfragen an diese Server senden	Standardmäßig ausgewählt. McAfee empfiehlt, diese Option ausgewählt zu lassen, da sie DNS-Abfragen möglicherweise beschleunigt, weil die Appliance die Abfragen nur an die angegebenen DNS-Server sendet. Wenn die Adresse unbekannt ist, werden Anfragen an die Root-DNS-Server im Internet gesendet. Wenn eine Antwort eingeht, empfängt die Appliance die Antwort und legt diese im Cache ab, sodass andere Server, die Abfragen an diesen DNS-Server senden, schneller eine Antwort erhalten können. Wenn Sie diese Option deaktivieren, versucht die Appliance zuerst, die Anfragen aufzulösen oder Abfragen an DNS-Server außerhalb Ihres Netzwerks zu senden.

Routing-Einstellungen

Option	Beschreibung
Netzwerkadresse	Geben Sie die Netzwerkadresse der Route ein.
Maske	Gibt an, wie viele Hosts sich in Ihrem Netzwerk befinden, beispielsweise 255.255.255.0.
Gateway	Gibt die IP-Adresse des Routers an, der als nächster Hop außerhalb des Netzwerks verwendet wird. Die Adresse 0.0.0.0 (IPv4) oder :: (IPv6) bedeutet, dass der Router über kein Standard-Gateway verfügt.
Messgröße	Gibt die Priorität an, die der Route beigemessen wird. Eine niedrige Zahl weist auf eine hohe Priorität der jeweiligen Route hin.
Neue Route/ Ausgewählte Routen löschen	Fügen Sie eine neue Route zur Tabelle hinzu, oder entfernen Sie Routen daraus. Mithilfe der Pfeile können Sie Routen in der Liste nach oben und unten verschieben. Die Routen werden auf Grundlage ihrer Metrik ausgewählt.
Dynamisches Routing aktivieren	Verwenden Sie diese Option nur im Modus "Transparenter Router". Wenn diese Option aktiviert ist, kann die Appliance: • Per Broadcast verbreitete Routing-Informationen empfangen, die über RIP (Standard) empfangen werden, und diese auf ihre Routing-Tabelle anwenden, sodass Sie Routing-Informationen, die bereits im Netzwerk vorhanden sind, nicht auf der Appliance duplizieren müssen • Routing-Informationen per Broadcast verbreiten, wenn statische Routen über RIP in der Benutzeroberfläche konfiguriert wurden

Seite "E-Mail-Konfiguration" (Benutzerdefinierte Einrichtung)

Hier werden die auf dieser Seite verfügbaren Optionen beschrieben.

E-Mail-Erstkonfiguration

Option	Beschreibung
Schutz vor potenziell unerwünschten Programme aktivieren...	Klicken Sie hier, um den Schutz vor potenziell unerwünschten Programmen zu aktivieren. Lesen Sie die Hinweise von McAfee zu den Auswirkungen, die das Aktivieren dieses Schutzes haben kann.
McAfee Global Threat Intelligence-Feedback aktivieren	Klicken Sie auf **Was ist das?**, um Informationen darüber zu erhalten, wie das Feedback genutzt wird, und um die McAfee-Datenschutzrichtlinien anzuzeigen.
SMTP-Verkehr scannen/ POP3-Verkehr scannen	Beide Protokolle sind standardmäßig ausgewählt. Heben Sie die Auswahl eines Protokolls auf, wenn es nicht gescannt werden soll.

Optionsbeschreibungen – Domänen, für die die Appliance E-Mails akzeptiert oder ablehnt

Verwenden Sie diese Optionen, um festzulegen, wie die Appliance E-Mails weiterleitet. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Domänen über **E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails** verwalten.

Option	Beschreibung
Domänenname/ Netzwerkadresse/ MX-Eintrag	Zeigt die Domänennamen, Platzhalter-Domänennamen, Netzwerkadressen und MX-Suchen an, von denen die Appliance E-Mails akzeptiert oder ablehnt.
Typ	• **Domänenname** – zum Beispiel `example.dom`. Wird von der Appliance verwendet, um die E-Mail-Adresse des Empfängers und die Verbindung mit einer Suche nach A-Einträgen zu vergleichen. • **Netzwerkadresse** – zum Beispiel `192.168.0.2/32` oder `192.168.0.0/24`. Wird von der Appliance verwendet, um die IP-Literal-E-Mail-Adresse des Empfängers, wie zum Beispiel `user@[192.168.0.2]`, oder die Verbindung zu vergleichen. • **MX-Eintrag-Suche** – zum Beispiel `example.dom`. Wird von der Appliance verwendet, um die Verbindung mit einer Suche nach MX-Einträgen zu vergleichen. • **Platzhalter-Domänenname** – zum Beispiel `*.example.dom`. Die Appliance verwendet diese Informationen nur, um die E-Mail-Adresse des Empfängers zu vergleichen.
Kategorie	• **Lokale Domäne** • **Zulässige Domäne** • **Verweigerte Domäne**

Option	Beschreibung
Domäne hinzufügen	Klicken Sie hier, um die Domänen anzugeben, die Nachrichten über die Appliance an den Empfänger weiterleiten können. Folgende Optionen stehen zur Auswahl: • **Lokale Domäne** – Hierbei handelt es sich um die Domänen oder Netzwerke, für die E-Mails zur Zustellung akzeptiert werden. Zur Erleichterung Ihrer Arbeit stehen die Optionen **Listen importieren** und **Listen exportieren** zur Verfügung, mit denen Sie eine Liste der Namen Ihrer lokalen Domänen importieren können. McAfee empfiehlt, alle Domänen oder Netzwerke hinzuzufügen, die als lokale Domänen Nachrichten weiterleiten dürfen. • **Zulässige Domäne** – E-Mails werden akzeptiert. Verwenden Sie "Zulässige Domänen" zum Verwalten von Ausnahmen. • **Verweigerte Domäne** – E-Mails werden abgelehnt. Verwenden Sie "Verweigerte Domänen" zum Verwalten von Ausnahmen. Bewegen Sie den Mauszeiger auf das Feld, damit das empfohlene Format angezeigt wird. Sie müssen mindestens eine lokale Domäne einrichten.
MX-Suche hinzufügen	Klicken Sie hier, um eine Domäne anzugeben, die von der Appliance zum Identifizieren aller Mailserver-IP-Adressen verwendet wird, von denen sie Nachrichten zustellt.
Ausgewählte Elemente löschen	Entfernt das ausgewählte Element aus der Tabelle. Sie müssen die Änderungen übernehmen, bevor das Element vollständig aus der Appliance-Konfiguration entfernt wird.

Optionsbeschreibungen – Domänen-Routing

Konfigurieren Sie die Hosts, die die Appliance zum Weiterleiten von E-Mails nutzt. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Domänen über **E-Mail | E-Mail-Konfiguration | Senden von E-Mails** verwalten.

Option	Beschreibung
Domänenname / Netzwerkadresse/ MX-Eintrag	Zeigt eine Liste der Domänen an. In der Liste können Sie bestimmte Relays/mehrere Relays angeben, die zum Zustellen von Nachrichten verwendet werden können, die für bestimmte Domänen bestimmt sind. Domänen können anhand von exakten Übereinstimmungen oder Musterübereinstimmungen wie z. B. ***.example.com** identifiziert werden. Sie können für eine Domäne mehrere Relays angeben, indem Sie sie durch ein Leerzeichen voneinander trennen. Falls das erste Mail-Relay E-Mail akzeptiert, werden alle E-Mail-Nachrichten an dieses erste Relay gesendet. Sobald das Relay keine E-Mails mehr akzeptiert, werden die nachfolgenden E-Mails an das nächste Relay in der Liste gesendet.
Typ	• **Domänenname** – zum Beispiel `example.dom`. Wird von der Appliance verwendet, um die E-Mail-Adresse des Empfängers und die Verbindung mit einer Suche nach A-Einträgen zu vergleichen. • **Netzwerkadresse** – zum Beispiel `192.168.0.2/32` oder `192.168.0.0/24`. Wird von der Appliance verwendet, um die IP-Literal-E-Mail-Adresse des Empfängers, wie zum Beispiel `user@[192.168.0.2]`, oder die Verbindung zu vergleichen. • **MX-Eintrag-Suche** – zum Beispiel `example.dom`. Wird von der Appliance verwendet, um die Verbindung mit einer Suche nach MX-Einträgen zu vergleichen. • **Platzhalter-Domänenname** – zum Beispiel `*.example.dom`. Die Appliance verwendet diese Informationen nur, um die E-Mail-Adresse des Empfängers zu vergleichen.
Kategorie	• **Lokale Domäne** • **Zulässige Domäne** • **Verweigerte Domäne**
Relay-Liste hinzufügen	Klicken Sie hier, um die Tabelle **Bekannte Domänen und Relay-Hosts** mit einer Liste der Host-Namen oder IP-Adressen für die Zustellung zu füllen. Die Zustellung wird in der angegebenen Reihenfolge versucht, es sei denn, Sie wählen die Option **Round-Robin der obenstehenden Hosts**, durch die die Last zwischen den angegebenen Hosts verteilt wird. Host-Namen/IP-Adressen können eine Port-Nummer enthalten.
MX-Suche hinzufügen	Klicken Sie hier, um die Tabelle **Bekannte Domänen und Relay-Hosts** mithilfe einer Suche nach MX-Einträgen, bei der die IP-Adressen für die Zustellung ermittelt werden, zu füllen. Es wird versucht, eine Zustellung an die Host-Namen durchzuführen, die von der MX-Suche zurückgegeben wurden. Dabei wird die durch den DNS-Server vorgegebene Reihenfolge der Prioritäten eingehalten.
Ausgewählte Elemente löschen	Entfernt das ausgewählte Element aus der Tabelle. Sie müssen die Änderungen übernehmen, bevor das Element vollständig aus der Appliance-Konfiguration entfernt wird.
DNS-Suche für Domänen, die oben nicht aufgeführt sind, aktivieren	Ist diese Option ausgewählt, verwendet die Appliance stattdessen DNS, um E-Mail-Nachrichten an andere, nicht näher spezifizierte Domänen weiterzuleiten. Bei der DNS-Zustellung wird versucht, eine Suche nach MX-Einträgen durchzuführen. Wenn keine MX-Einträge vorhanden sind, wird nach A-Einträgen gesucht. Wenn Sie das Kontrollkästchen deaktivieren, stellt die Appliance E-Mail nur an Domänen zu, die unter **Bekannte Domänen und Relay-Hosts** angegeben sind.

Seite "Zeiteinstellungen"

Auf dieser Seite können Sie die Uhrzeit und das Datum sowie sämtliche Details für die Verwendung von NTP (Network Time Protocol) festlegen.

Option	Beschreibung
Zeitzone der Appliance	Gibt die Zeitzone der Appliance an. Wenn in Ihrer Region Sommer- und Winterzeit gelten, müssen Sie die Zeitzone zweimal im Jahr ändern.
Appliance-Zeit (UTC)	Gibt das Datum und die UTC-Zeit für die Appliance an. Um das Datum festzulegen, klicken Sie auf das Kalendersymbol. Sie können die UTC-Zeit von Websites ablesen, z. B. von http://www.worldtimeserver.com.
Jetzt einstellen	Wenn Sie hierauf klicken, werden das Datum und die UTC-Zeit, die Sie in dieser Zeile ausgewählt haben, übernommen.
Client-Zeit	Zeigt die Zeit entsprechend dem Client-Computer an, von dem aus Ihr Browser derzeit mit der Appliance verbunden ist.
Appliance mit Client synchronisieren	Bei Auswahl übernimmt die Zeit unter **Appliance-Zeit (UTC)** sofort den Wert aus **Client-Zeit**. Sie können dieses Kontrollkästchen als Alternative verwenden, um manuell die **Appliance-Zeit (UTC)** einzustellen. Die Appliance errechnet die UTC-Zeit basierend auf der Zeitzone, die sie im Client-Browser findet. Stellen Sie sicher, dass der Client-Computer Sommer- und Winterzeit berücksichtigt. Um die Einstellung in Microsoft Windows zu finden, klicken Sie mit der rechten Maustaste in die untere rechte Ecke des Bildschirms.
NTP aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten von einem angegebenen Server oder einem Netzwerk-Broadcast. NTP synchronisiert die Uhrzeiten unter den Geräten in einem Netzwerk. Einige Internet-Dienstanbieter bieten einen Uhrzeitdienst an. Da NTP-Nachrichten nicht häufig versendet werden, beeinträchtigen sie die Leistung der Appliance nicht wesentlich.
NTP-Client-Broadcasts aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten nur von Netzwerk-Broadcasts. Diese Methode ist hilfreich, wenn das Netzwerk ausgelastet ist, aber anderen Geräten im Netzwerk vertrauen muss. Wenn diese Option nicht ausgewählt ist, akzeptiert NTP Nachrichten nur von Servern, die in der Liste angegeben sind.
NTP-Server	Zeigt die Netzwerkadresse oder einen Domänennamen eines oder mehrerer NTP-Server an, die die Appliance verwendet. Z. B. time.nist.gov. Wenn Sie mehrere Server angeben, prüft die Appliance jede NTP-Nachricht, um die richtige Uhrzeit zu bestimmen.
Neuer Server	Geben Sie die IP-Adresse eines neuen NTP-Servers ein.

Seite "Kennwort"

Verwenden Sie diese Seite, um ein Kennwort für die Appliance anzugeben.

Ein sicheres Kennwort besteht aus Buchstaben und Ziffern. Sie können bis zu 15 Zeichen eingeben.

Option	Beschreibung
Benutzer-ID	Diese lautet **admin**. Sie können später weitere Benutzer hinzufügen.
Kennwort	Gibt das neue Kennwort an. Ändern Sie das Kennwort baldmöglichst, damit Ihre Appliance geschützt bleibt. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen. Das ursprüngliche Standardkennwort lautet **password**.

Seite "Zusammenfassung"

Zeigen Sie eine Zusammenfassung der Einstellungen an, die Sie für Netzwerkverbindungen und das Scannen des E-Mail-Verkehrs vorgenommen haben.

Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen.

Verwenden Sie die hier angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: *https://192.168.200.10*. Die Adresse beginnt mit https und nicht mit http.



Wenn Sie Ihr McAfee® Email Gateway für Secure Web Mail konfiguriert haben, müssen Sie auf die Appliance über den Port 10443 zugreifen. Im oben angegebenen Beispiel würden Sie demzufolge *https://192.168.200.10:10443* eingeben.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **admin** und das Kennwort ein, das Sie auf der Seite **Kennwort** angegeben haben.

Tabelle 3-2 Grundlegende Einstellungen

Option	Beschreibung
	Der Wert entspricht bewährten Praktiken.
	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

Wiederherstellung aus einer Datei

In diesem Abschnitt erfahren Sie, welchen Zweck die Wiederherstellung aus einer Datei hat.

Wenn Sie Ihr Gerät über den **Setup-Assistenten** innerhalb der Benutzeroberfläche konfigurieren, können Sie mithilfe der Option **Aus Datei wiederherstellen** zuvor gespeicherte Konfigurationsdaten importieren und auf Ihr Gerät übernehmen. Nachdem diese Daten importiert wurden, können Sie Änderungen vornehmen, bevor Sie die Konfiguration anwenden.



Die Option **Aus Datei wiederherstellen** ist in der **Konfigurationskonsole** nicht verfügbar. Zum Verwenden dieser Option müssen Sie sich beim McAfee Email Gateway anmelden und **Aus Datei wiederherstellen** aus dem Menü **System** | **Setup-Assistent** auswählen.

Nachdem die Konfigurationsdaten importiert wurden, werden die Optionen der **Benutzerdefinierten Einrichtung** im **Setup-Assistenten** angezeigt (siehe *Durchführen der benutzerdefinierten Einrichtung*). Alle importierten Optionen werden auf den Assistentenseiten angezeigt, sodass Sie die Möglichkeit zum Vornehmen von Änderungen haben, bevor Sie die Konfiguration übernehmen.

Bei Verwendung der Option **Aus Datei wiederherstellen** enthält der Assistent die folgenden Seiten:

- **Konfigurationsdatei importieren**
- **Wiederherzustellende Werte**

Nachdem diese Informationen geladen wurden, werden die Seiten der **Benutzerdefinierten Einrichtung** angezeigt, in denen Sie weitere Änderungen vornehmen können, bevor Sie die neue Konfiguration übernehmen:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **DNS und Routing**
- **Zeiteinstellungen**
- **Kennwort**
- **Zusammenfassung**

Seite "Grundlegende Einstellungen" (Benutzerdefinierte Einrichtung)

Im Assistenten "Benutzerdefinierte Einrichtung" geben Sie auf dieser Seite die grundlegenden Einstellungen der Appliance an.

Die Appliance versucht, Ihnen einige Informationen zur Verfügung zu stellen, und zeigt die Informationen gelb markiert an. Um diese Informationen zu ändern, klicken Sie, und geben Sie sie erneut ein.

Option	Beschreibung
Cluster-Modus	Definiert die Optionen, die auf der Seite **Cluster-Verwaltung** des Setup-Assistenten erscheinen. • **Aus** – Dies ist eine Standard-Appliance. • **Cluster-Scanner** – Die Appliance empfängt ihre Scan-Arbeit von einer Master-Appliance. • **Cluster-Master** – Die Appliance steuert die Scan-Arbeit verschiedener anderer Appliances. • **Cluster-Failover** – Falls der Master ausfällt, steuert diese Appliance stattdessen die Scan-Arbeit.
Gerätename	Gibt einen Namen an, z. B. Appliance1.
Domänenname	Gibt einen Domänennamen an, z. B. domaene1.com.
Standard-Gateway	Gibt eine IPv4-Adresse an, z. B. 198.168.10.1. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Nächster Router	Gibt eine IPv6-Adresse an, z. B. FD4A:A1B2:C3D4::1.
Netzwerkschnittstelle	Wird verfügbar, wenn Sie das Feld **Nächster Router** für IPv6 festlegen.

Seite "Cluster-Verwaltung"

Auf dieser Seite können Sie die Lastverteilung im Cluster konfigurieren.



Abhängig davon, welchen Cluster-Modus Sie auf der Seite **Grundlegende Einstellungen** ausgewählt haben, ändern sich die auf der Seite **Cluster-Verwaltung** angezeigten Optionen.

Konfiguration der Cluster-Verwaltung (Standard-Appliance)

Nicht verwenden. Die Cluster-Verwaltung ist deaktiviert.

Cluster-Verwaltung (Cluster-Scanner)

Option	Beschreibung
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.

Cluster-Verwaltung (Cluster-Master)



Im Modus "Expliziter Proxy" oder "Transparenter Router" können Sie das Failover zwischen zwei Appliances in einem Cluster aktivieren, indem Sie dieser Appliance eine virtuelle IP-Adresse zuweisen und eine andere Appliance als Cluster-Failover-Appliance mit derselben virtuellen Adresse konfigurieren. Im Modus "Transparente Bridge" erreichen Sie dies, indem Sie eine hohe STP-Priorität für diese Appliance einrichten und eine andere Appliance als Cluster-Failover-Appliance mit einer geringeren STP-Priorität konfigurieren.

Option	Beschreibung
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. Wenn Sie in einem Appliance-Cluster nur über eine Master- und eine Failover-Appliance verfügen, die beide für das Scannen des Datenverkehrs konfiguriert sind, sendet die Master-Appliance die meisten Verbindungen zum Scannen an die Failover-Appliance.

Optionsbeschreibungen – Erweiterte Einstellungen für Scan-Geräte

Verwenden Sie diesen Bereich für die detaillierte Kontrolle der verbundenen Scan-Geräte. Sie können die Geräte auch für die gemeinsame Nutzung von Festplattenspeicher zur Speicherung von Secure Web Mail-Nachrichten konfigurieren. Geräte in einem Cluster werden über ihre MAC-Adressen (Media Access Control) identifiziert. Wenn Sie der Tabelle eine MAC-Adresse hinzufügen, können Sie diese deaktivieren, sodass keine Scan-Anfragen an das Gerät gesendet werden. Außerdem können Sie Festplattenspeicher gemeinsam nutzen.

Option	Beschreibung
MAC-Adresse	Gibt die MAC-Adresse (Media Access Control) des Geräts mit 12 Hexadezimalstellen im folgenden Format an: A1:B2:C3:D4:E5:F6.
Deaktiviert	Wählen Sie diese Option, wenn Sie dieses Gerät aus der Gruppe der Scan-Geräte entfernen möchten.
MAC-Adresse hinzufügen	Klicken Sie auf diese Schaltfläche, wenn Sie die MAC-Adresse eines neuen Geräts hinzufügen möchten.
MAC-Adressen verwalten	Öffnet das Dialogfeld "MAC-Adressen", in dem Sie die Liste der verfügbaren MAC-Adressen verwalten können.



Obwohl Sie dieser Tabelle die MAC-Adressen der Management- und Failover-Geräte hinzufügen können, können diese nicht deaktiviert werden, da sie immer Festplattenspeicher für Secure Web Mail-Nachrichten bereitstellen.

Cluster-Verwaltung (Cluster-Failover)

Option	Beschreibung
Für Lastenausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an. Bietet eine Liste aller einer Appliance zugewiesenen Subnetze.
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. Wenn Sie in einem Appliance-Cluster nur über eine Master- und eine Failover-Appliance verfügen, die beide für das Scannen des Datenverkehrs konfiguriert sind, sendet die Master-Appliance die meisten Verbindungen zum Scannen an die Failover-Appliance.

Seite "DNS und Routing"

Verwenden Sie diese Seite, um die Verwendung von DNS und Routen durch die Appliance zu konfigurieren.

DNS-Server (Domain Name System) übersetzen die Namen von Netzwerkgeräten in IP-Adressen (und umgekehrt), d. h., sie ordnen die Namen und Adressen einander zu. Die Appliance sendet in der hier aufgeführten Reihenfolge Anfragen an DNS-Server.

DNS-Server-Adressen

Option	Beschreibung
Server-Adresse	Zeigt die IP-Adressen der DNS-Server an. Beim ersten Server in der Liste muss es sich um den schnellsten bzw. zuverlässigsten Server handeln. Falls der erste Server die Anforderung nicht auflösen kann, nimmt die Appliance Kontakt mit dem zweiten Server auf. Falls keiner der Server in der Liste die Anforderung auflösen kann, leitet die Appliance die Anforderung an die DNS-Root-Namenserver im Internet weiter. Geben Sie die IP-Adresse eines lokalen Geräts mit Namensauflösungsfunktion an, wenn DNS-Suchen (in der Regel auf Port 53) von der Firewall verhindert werden.
Neuer Server/ Ausgewählte Server löschen	Fügt einen neuen Server zur Liste hinzu oder entfernt einen Server, beispielsweise, wenn Sie einen Server aufgrund von Netzwerkänderungen außer Betrieb setzen müssen.
Nur Anfragen an diese Server senden	Standardmäßig ausgewählt. McAfee empfiehlt, diese Option ausgewählt zu lassen, da sie DNS-Abfragen möglicherweise beschleunigt, weil die Appliance die Abfragen nur an die angegebenen DNS-Server sendet. Wenn die Adresse unbekannt ist, werden Anfragen an die Root-DNS-Server im Internet gesendet. Wenn eine Antwort eingeht, empfängt die Appliance die Antwort und legt diese im Cache ab, sodass andere Server, die Abfragen an diesen DNS-Server senden, schneller eine Antwort erhalten können. Wenn Sie diese Option deaktivieren, versucht die Appliance zuerst, die Anfragen aufzulösen oder Abfragen an DNS-Server außerhalb Ihres Netzwerks zu senden.

Routing-Einstellungen

Option	Beschreibung
Netzwerkadresse	Geben Sie die Netzwerkadresse der Route ein.
Maske	Gibt an, wie viele Hosts sich in Ihrem Netzwerk befinden, beispielsweise 255.255.255.0.

Option	Beschreibung
Gateway	Gibt die IP-Adresse des Routers an, der als nächster Hop außerhalb des Netzwerks verwendet wird. Die Adresse 0.0.0.0 (IPv4) oder :: (IPv6) bedeutet, dass der Router über kein Standard-Gateway verfügt.
Messgröße	Gibt die Priorität an, die der Route beigemessen wird. Eine niedrige Zahl weist auf eine hohe Priorität der jeweiligen Route hin.
Neue Route/ Ausgewählte Routen löschen	Fügen Sie eine neue Route zur Tabelle hinzu, oder entfernen Sie Routen daraus. Mithilfe der Pfeile können Sie Routen in der Liste nach oben und unten verschieben. Die Routen werden auf Grundlage ihrer Metrik ausgewählt.
Dynamisches Routing aktivieren	Verwenden Sie diese Option nur im Modus "Transparenter Router". Wenn diese Option aktiviert ist, kann die Appliance: • Per Broadcast verbreitete Routing-Informationen empfangen, die über RIP (Standard) empfangen werden, und diese auf ihre Routing-Tabelle anwenden, sodass Sie Routing-Informationen, die bereits im Netzwerk vorhanden sind, nicht auf der Appliance duplizieren müssen • Routing-Informationen per Broadcast verbreiten, wenn statische Routen über RIP in der Benutzeroberfläche konfiguriert wurden

Seite "Zeiteinstellungen"

Auf dieser Seite können Sie die Uhrzeit und das Datum sowie sämtliche Details für die Verwendung von NTP (Network Time Protocol) festlegen.

Option	Beschreibung
Zeitzone der Appliance	Gibt die Zeitzone der Appliance an. Wenn in Ihrer Region Sommer- und Winterzeit gelten, müssen Sie die Zeitzone zweimal im Jahr ändern.
Appliance-Zeit (UTC)	Gibt das Datum und die UTC-Zeit für die Appliance an. Um das Datum festzulegen, klicken Sie auf das Kalendersymbol. Sie können die UTC-Zeit von Websites ablesen, z. B. von http://www.worldtimeserver.com.
Jetzt einstellen	Wenn Sie hierauf klicken, werden das Datum und die UTC-Zeit, die Sie in dieser Zeile ausgewählt haben, übernommen.
Client-Zeit	Zeigt die Zeit entsprechend dem Client-Computer an, von dem aus Ihr Browser derzeit mit der Appliance verbunden ist.
Appliance mit Client synchronisieren	Bei Auswahl übernimmt die Zeit unter **Appliance-Zeit (UTC)** sofort den Wert aus **Client-Zeit**. Sie können dieses Kontrollkästchen als Alternative verwenden, um manuell die **Appliance-Zeit (UTC)** einzustellen. Die Appliance errechnet die UTC-Zeit basierend auf der Zeitzone, die sie im Client-Browser findet. Stellen Sie sicher, dass der Client-Computer Sommer- und Winterzeit berücksichtigt. Um die Einstellung in Microsoft Windows zu finden, klicken Sie mit der rechten Maustaste in die untere rechte Ecke des Bildschirms.
NTP aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten von einem angegebenen Server oder einem Netzwerk-Broadcast. NTP synchronisiert die Uhrzeiten unter den Geräten in einem Netzwerk. Einige Internet-Dienstanbieter bieten einen Uhrzeitdienst an. Da NTP-Nachrichten nicht häufig versendet werden, beeinträchtigen sie die Leistung der Appliance nicht wesentlich.
NTP-Client-Broadcasts aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten nur von Netzwerk-Broadcasts. Diese Methode ist hilfreich, wenn das Netzwerk ausgelastet ist, aber anderen Geräten im Netzwerk vertrauen muss. Wenn diese Option nicht ausgewählt ist, akzeptiert NTP Nachrichten nur von Servern, die in der Liste angegeben sind.

Option	Beschreibung
NTP-Server	Zeigt die Netzwerkadresse oder einen Domänennamen eines oder mehrerer NTP-Server an, die die Appliance verwendet. Z. B. time.nist.gov. Wenn Sie mehrere Server angeben, prüft die Appliance jede NTP-Nachricht, um die richtige Uhrzeit zu bestimmen.
Neuer Server	Geben Sie die IP-Adresse eines neuen NTP-Servers ein.

Seite "Kennwort"

Verwenden Sie diese Seite, um ein Kennwort für die Appliance anzugeben.

Ein sicheres Kennwort besteht aus Buchstaben und Ziffern. Sie können bis zu 15 Zeichen eingeben.

Option	Beschreibung
Benutzer-ID	Diese lautet **admin**. Sie können später weitere Benutzer hinzufügen.
Kennwort	Gibt das neue Kennwort an. Ändern Sie das Kennwort baldmöglichst, damit Ihre Appliance geschützt bleibt. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen. Das ursprüngliche Standardkennwort lautet **password**.

Seite "Zusammenfassung"

Zeigen Sie eine Zusammenfassung der Einstellungen an, die Sie für Netzwerkverbindungen und das Scannen des E-Mail-Verkehrs vorgenommen haben.

Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen.

Verwenden Sie die hier angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: *https://192.168.200.10*. Die Adresse beginnt mit https und nicht mit http.



Wenn Sie Ihr McAfee® Email Gateway für Secure Web Mail konfiguriert haben, müssen Sie auf die Appliance über den Port 10443 zugreifen. Im oben angegebenen Beispiel würden Sie demzufolge *https://192.168.200.10:10443* eingeben.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **admin** und das Kennwort ein, das Sie auf der Seite **Kennwort** angegeben haben.

Tabelle 3-3 Grundlegende Einstellungen

Option	Beschreibung
	Der Wert entspricht bewährten Praktiken.
	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

Setup im Modus 'Nur Verschlüsselung'

In diesem Abschnitt erfahren Sie, welchen Zweck die Einrichtungsoptionen im Modus "Nur Verschlüsselung" haben.

In kleinen bis mittleren Organisationen genügt es häufig, dasselbe McAfee Email Gateway für E-Mail-Scanning- und E-Mail-Verschlüsselungs-Tasks zu verwenden.

Wenn Sie jedoch in einem größeren Unternehmen bzw. in einer Branche arbeiten, wo die Zustellung des gesamten oder eines überwiegenden Teils des E-Mail-Aufkommens auf eine sichere Weise erfolgen muss, kann es empfehlenswert sein, eine oder mehrere McAfee Email Gateway-Appliances als eigenständige Verschlüsselungs-Server einzurichten.

Unter diesen Umständen bieten Ihnen die Optionen für das **Setup im Modus "Nur Verschlüsselung"** innerhalb des **Setup-Assistenten** die relevanten Einstellungen, die für den Betrieb im Modus "Nur Verschlüsselung" erforderlich sind.

Für das **Setup im Modus "Nur Verschlüsselung"** enthält der Assistent die folgenden Seiten:

Seite "E-Mail-Konfiguration" (Setup im Modus 'Nur Verschlüsselung')

Definieren Sie, wie die Appliance E-Mail weiterleitet, und konfigurieren Sie die Hosts, die die Appliance für das Routen von E-Mails verwenden soll.

Domänen, für die die Appliance E-Mails akzeptiert oder ablehnt



Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Domänen über **E-Mail** | **E-Mail-Konfiguration** | **Empfangen von E-Mails** verwalten.

Option	Beschreibung
Domänenname / Netzwerkadresse/ MX-Eintrag	Zeigt die Domänennamen, Platzhalter-Domänennamen, Netzwerkadressen und MX-Suchen an, von denen die Appliance E-Mails akzeptiert oder ablehnt.
Typ	• **Domänenname** – Beispiel: example.dom. Wird von der Appliance verwendet, um die E-Mail-Adresse des Empfängers und die Verbindung mit einer Suche nach A-Einträgen zu vergleichen. • **Netzwerkadresse** – Beispiel: 192.168.0.2/32 oder 192.168.0.0/24. Die Appliance verwendet diese Adresse, um die IP-Literal-E-Mail-Adresse des Empfängers, wie zum Beispiel user@[192.168.0.2], oder die Verbindung zu vergleichen. • **MX-Eintrag-Suche** – Beispiel: example.dom. Wird von der Appliance verwendet, um die Verbindung mit einer MX-Eintrag-Suche zu vergleichen. • **Platzhalter-Domänenname** – Beispiel: *.example.dom. Die Appliance verwendet diese Informationen, um die E-Mail-Adressen der Empfänger zu vergleichen.
Kategorie	• **Lokale Domäne** • **Zulässige Domäne** • **Verweigerte Domäne**

Option	Beschreibung
Domäne hinzufügen	Klicken Sie hier, um die Domänen anzugeben, die Nachrichten über die Appliance an den Empfänger weiterleiten können. Folgende Optionen stehen zur Auswahl: • **Lokale Domäne** – Hierbei handelt es sich um die Domänen oder Netzwerke, für die E-Mails zur Zustellung akzeptiert werden. Zur Erleichterung Ihrer Arbeit stehen die Optionen **Listen importieren** und **Listen exportieren** zur Verfügung, mit denen Sie eine Liste der Namen Ihrer lokalen Domänen importieren können. McAfee empfiehlt, alle Domänen oder Netzwerke hinzuzufügen, die als lokale Domänen Nachrichten weiterleiten dürfen. • **Zulässige Domäne** – E-Mails werden akzeptiert. Verwenden Sie "Zulässige Domänen" zum Verwalten von Ausnahmen. • **Verweigerte Domäne** – E-Mails werden abgelehnt. Verwenden Sie "Verweigerte Domänen" zum Verwalten von Ausnahmen. Bewegen Sie den Mauszeiger auf das Feld, damit das empfohlene Format angezeigt wird. Sie müssen mindestens eine lokale Domäne einrichten.
MX-Suche hinzufügen	Klicken Sie hier, um eine Domäne anzugeben, die von der Appliance zum Identifizieren aller Mailserver-IP-Adressen verwendet wird, von denen sie Nachrichten zustellt.
Ausgewählte Elemente löschen	Entfernt das ausgewählte Element aus der Tabelle. Sie müssen die Änderungen übernehmen, bevor das Element vollständig aus der Appliance-Konfiguration entfernt wird.

Domänen-Routing



Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Domänen über **E-Mail** \| **E-Mail-Konfiguration** \| **Senden von E-Mail** verwalten.

Option	Beschreibung
Domänen	Zeigt eine Liste der Domänen an.
Typ	• **Domänenname** – Beispiel: example.dom. Wird von der Appliance verwendet, um die E-Mail-Adresse des Empfängers und die Verbindung mit einer Suche nach A-Einträgen zu vergleichen. • **Netzwerkadresse** – Beispiel: 192.168.0.2/32 oder 192.168.0.0/24. Die Appliance verwendet diese Adresse, um die IP-Literal-E-Mail-Adresse des Empfängers, wie zum Beispiel user@[192.168.0.2], oder die Verbindung zu vergleichen. • **MX-Eintrag-Suche** – Beispiel: example.dom. Wird von der Appliance verwendet, um die Verbindung mit einer MX-Eintrag-Suche zu vergleichen. • **Platzhalter-Domänenname** – Beispiel: *.example.dom. Die Appliance verwendet diese Informationen, um die E-Mail-Adressen der Empfänger zu vergleichen.
Relay-Liste/ MX-Eintrag	Zeigt die **Relay-Liste** oder den **MX-Eintrag** für die ausgewählte Domäne an.
Relay-Liste hinzufügen	Klicken Sie hier, um die Tabelle **Bekannte Domänen und Relay-Hosts** mit einer Liste der Host-Namen oder IP-Adressen für die Zustellung zu füllen. Die Zustellung wird in der angegebenen Reihenfolge versucht, es sei denn, Sie wählen die Option **Round-Robin der obenstehenden Hosts**, durch die die Last zwischen den angegebenen Hosts verteilt wird. Host-Namen/IP-Adressen können eine Port-Nummer enthalten.

Option	Beschreibung
MX-Suche hinzufügen	Klicken Sie hier, um die Tabelle **Bekannte Domänen und Relay-Hosts** mithilfe einer Suche nach MX-Einträgen, bei der die IP-Adressen für die Zustellung ermittelt werden, zu füllen. Es wird versucht, eine Zustellung an die Host-Namen durchzuführen, die von der MX-Suche zurückgegeben wurden. Dabei wird die durch den DNS-Server vorgegebene Reihenfolge der Prioritäten eingehalten.
Ausgewählte Elemente löschen	Entfernt das ausgewählte Element aus der Tabelle. Sie müssen die Änderungen übernehmen, bevor das Element vollständig aus der Appliance-Konfiguration entfernt wird.
DNS-Suche für Domänen, die oben nicht aufgeführt sind, aktivieren	Ist diese Option ausgewählt, verwendet die Appliance stattdessen DNS, um E-Mail-Nachrichten an andere, nicht näher spezifizierte Domänen weiterzuleiten. Bei der DNS-Zustellung wird versucht, eine Suche nach MX-Einträgen durchzuführen. Wenn keine MX-Einträge vorhanden sind, wird nach A-Einträgen gesucht. Wenn Sie das Kontrollkästchen deaktivieren, stellt die Appliance E-Mails nur an Domänen zu, die angegeben sind unter: **Bekannte Domänen und Relay-Hosts** .

Seite "Grundlegende Einstellungen" (Setup im Modus 'Nur Verschlüsselung')

Auf dieser Seite geben Sie im Assistenten "Setup im Modus 'Nur Verschlüsselung'" die grundlegenden Einstellungen der Appliance an.

Die Appliance versucht, Ihnen einige Informationen zur Verfügung zu stellen, und zeigt die Informationen gelb markiert an. Um diese Informationen zu ändern, klicken Sie, und geben Sie sie erneut ein.

Option	Beschreibung
Cluster-Modus	Definiert die Optionen, die auf der Seite **Cluster-Verwaltung** des Setup-Assistenten erscheinen. • **Aus** – Dies ist eine Standard-Appliance. • **Cluster-Scanner** – Die Appliance empfängt ihre Scan-Arbeit von einer Master-Appliance. • **Cluster-Master** – Die Appliance steuert die Scan-Arbeit verschiedener anderer Appliances. • **Cluster-Failover** – Falls der Master ausfällt, steuert diese Appliance stattdessen die Scan-Arbeit.
Gerätename	Gibt einen Namen an, z. B. Appliance1.
Domänenname	Gibt einen Domänennamen an, z. B. domaene1.com.
Standard-Gateway	Gibt eine IPv4-Adresse an, z. B. 198.168.10.1. Sie können später testen, ob die Appliance mit diesem Server kommunizieren kann.
Nächster Router	Gibt eine IPv6-Adresse an, z. B. FD4A:A1B2:C3D4::1.
Netzwerkschnittstelle	Wird verfügbar, wenn Sie das Feld "Nächster Router" für IPv6 festlegen.
Management-Port auswählen	Gibt den Port an, über den das Gateway verwaltet wird. Standardmäßig verwendet McAfee Email Gateway den Port 10443.

Seite "Netzwerkeinstellungen" (Setup im Modus 'Nur Verschlüsselung')

Verwenden Sie diese Optionen, um die IP-Adresse und die Netzwerkgeschwindigkeiten für McAfee Email Gateway anzuzeigen, das als reine Verschlüsselungs-Appliance fungiert. Sie können IPv4- und IPv6-Adressen verwenden, entweder separat oder zusammen.

Vergeben Sie neue IP-Adressen für die Appliance und deaktivieren Sie die standardmäßigen IP-Adressen, um doppelte IP-Adressen im Netzwerk zu vermeiden und um Hacker abzuhalten. Die IP-Adressen müssen eindeutig und für Ihr Netzwerk geeignet sein. Geben Sie so viele IP-Adressen wie erforderlich an.

Option	Beschreibung
<mode>	Der Betriebsmodus, den Sie während der Installation oder im Setup-Assistenten festlegen.
Netzwerkschnittstelle 1	Wird erweitert und zeigt die IP-Adresse und die Netzmaske für die Netzwerkschnittstelle 1, den Autonegotiation-Status und die MTU-Größe an.
Netzwerkschnittstelle 2	Wird erweitert und zeigt die IP-Adresse und die Netzmaske für die Netzwerkschnittstelle 2, den Autonegotiation-Status und die MTU-Größe an.
Netzwerkeinstellungen ändern	Klicken Sie hier, um den Netzwerkschnittstellen-Assistenten zu öffnen, um die IP-Adresse und die Adaptereinstellungen für NIC 1 und NIC 2 anzugeben und den ausgewählten Betriebsmodus zu ändern.
Netzwerkschnittstellenlayout anzeigen	Klicken Sie hier, um das <?> zu sehen, das mit LAN1, LAN2 und der Out-of-Band-Schnittstelle verknüpft ist.

Seite "Cluster-Verwaltung" (Setup im Modus 'Nur Verschlüsselung')

Auf dieser Seite können Sie den Lastausgleich konfigurieren.



Abhängig davon, welchen Cluster-Modus Sie auf der Seite **Grundlegende Einstellungen** ausgewählt haben, ändern sich die auf der Seite **Cluster-Verwaltung** angezeigten Optionen.

Konfiguration der Cluster-Verwaltung (Standard-Appliance)

Nicht verwenden. Die Cluster-Verwaltung ist deaktiviert.

Cluster-Verwaltung (Cluster-Scanner)

Option	Beschreibung
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.

Cluster-Verwaltung (Cluster-Master)



Im Modus "Expliziter Proxy" oder "Transparenter Router" können Sie das Failover zwischen zwei Appliances in einem Cluster aktivieren, indem Sie dieser Appliance eine virtuelle IP-Adresse zuweisen und eine andere Appliance als Cluster-Failover-Appliance mit derselben virtuellen Adresse konfigurieren. Im Modus "Transparente Bridge" erreichen Sie dies, indem Sie eine hohe STP-Priorität für diese Appliance einrichten und eine andere Appliance als Cluster-Failover-Appliance mit einer geringeren STP-Priorität konfigurieren.

Option	Beschreibung
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.
Für Lastausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. Wenn Sie in einem Appliance-Cluster nur über eine Master- und eine Failover-Appliance verfügen, die beide für das Scannen des Datenverkehrs konfiguriert sind, sendet die Master-Appliance die meisten Verbindungen zum Scannen an die Failover-Appliance.

Cluster-Verwaltung (Cluster-Failover)

Option	Beschreibung
Für Lastausgleich zu verwendende Adresse	Gibt die Appliance-Adresse an. Bietet eine Liste aller einer Appliance zugewiesenen Subnetze.
Cluster-Kennung	Wenn Sie mehrere Cluster oder McAfee Content Security Blade Server im selben Subnetz betreiben, weisen Sie jedem Cluster eine andere **Cluster-Kennung** zu, damit es keine Konflikte zwischen den Clustern gibt. Der zulässige Bereich ist 0-255.
Scannen auf dieser Appliance aktivieren	Wenn diese Option nicht ausgewählt ist, verteilt diese Appliance die gesamte Scan-Arbeitslast auf die Scan-Appliances. Wenn Sie in einem Appliance-Cluster nur über eine Master- und eine Failover-Appliance verfügen, die beide für das Scannen des Datenverkehrs konfiguriert sind, sendet die Master-Appliance die meisten Verbindungen zum Scannen an die Failover-Appliance.

Seite "DNS und Routing" (Setup im Modus 'Nur Verschlüsselung')

Verwenden Sie diese Seite, um die Verwendung von DNS und Routen durch die Appliance zu konfigurieren.

DNS-Server (Domain Name System) übersetzen die Namen von Netzwerkgeräten in IP-Adressen (und umgekehrt), d. h., sie ordnen die Namen und Adressen einander zu. Die Appliance sendet in der hier aufgeführten Reihenfolge Anfragen an DNS-Server.

DNS-Server-Adressen

Option	Beschreibung
Server-Adresse	Zeigt die IP-Adressen der DNS-Server an. Beim ersten Server in der Liste muss es sich um den schnellsten bzw. zuverlässigsten Server handeln. Falls der erste Server die Anforderung nicht auflösen kann, nimmt die Appliance Kontakt mit dem zweiten Server auf. Falls keiner der Server in der Liste die Anforderung auflösen kann, leitet die Appliance die Anforderung an die DNS-Root-Namenserver im Internet weiter. Geben Sie die IP-Adresse eines lokalen Geräts mit Namensauflösungsfunktion an, wenn DNS-Suchen (in der Regel auf Port 53) von der Firewall verhindert werden.
Neuer Server/ Ausgewählte Server löschen	Fügt einen neuen Server zur Liste hinzu oder entfernt einen Server, beispielsweise, wenn Sie einen Server aufgrund von Netzwerkänderungen außer Betrieb setzen müssen.
Nur Anfragen an diese Server senden	Standardmäßig ausgewählt. McAfee empfiehlt, diese Option ausgewählt zu lassen, da sie DNS-Abfragen möglicherweise beschleunigt, weil die Appliance die Abfragen nur an die angegebenen DNS-Server sendet. Wenn die Adresse unbekannt ist, werden Anfragen an die Root-DNS-Server im Internet gesendet. Wenn eine Antwort eingeht, empfängt die Appliance die Antwort und legt diese im Cache ab, sodass andere Server, die Abfragen an diesen DNS-Server senden, schneller eine Antwort erhalten können. Wenn Sie diese Option deaktivieren, versucht die Appliance zuerst, die Anfragen aufzulösen oder Abfragen an DNS-Server außerhalb Ihres Netzwerks zu senden.

Routing-Einstellungen

Option	Beschreibung
Netzwerkadresse	Geben Sie die Netzwerkadresse der Route ein.
Maske	Gibt an, wie viele Hosts sich in Ihrem Netzwerk befinden, beispielsweise 255.255.255.0.
Gateway	Gibt die IP-Adresse des Routers an, der als nächster Hop außerhalb des Netzwerks verwendet wird. Die Adresse 0.0.0.0 (IPv4) oder :: (IPv6) bedeutet, dass der Router über kein Standard-Gateway verfügt.
Messgröße	Gibt die Priorität an, die der Route beigemessen wird. Eine niedrige Zahl weist auf eine hohe Priorität der jeweiligen Route hin.
Neue Route/ Ausgewählte Routen löschen	Fügen Sie eine neue Route zur Tabelle hinzu, oder entfernen Sie Routen daraus. Mithilfe der Pfeile können Sie Routen in der Liste nach oben und unten verschieben. Die Routen werden auf Grundlage ihrer Metrik ausgewählt.
Dynamisches Routing aktivieren	Verwenden Sie diese Option nur im Modus "Transparenter Router". Wenn diese Option aktiviert ist, kann die Appliance: • Per Broadcast verbreitete Routing-Informationen empfangen, die über RIP (Standard) empfangen werden, und diese auf ihre Routing-Tabelle anwenden, sodass Sie Routing-Informationen, die bereits im Netzwerk vorhanden sind, nicht auf der Appliance duplizieren müssen. • Routing-Informationen per Broadcast verbreiten, wenn statische Routen über RIP in der Benutzeroberfläche konfiguriert wurden.

Seite "Zeiteinstellungen"

Auf dieser Seite können Sie die Uhrzeit und das Datum sowie sämtliche Details für die Verwendung von NTP (Network Time Protocol) festlegen.

Option	Beschreibung
Zeitzone der Appliance	Gibt die Zeitzone der Appliance an. Wenn in Ihrer Region Sommer- und Winterzeit gelten, müssen Sie die Zeitzone zweimal im Jahr ändern.
Appliance-Zeit (UTC)	Gibt das Datum und die UTC-Zeit für die Appliance an. Um das Datum festzulegen, klicken Sie auf das Kalendersymbol. Sie können die UTC-Zeit von Websites ablesen, z. B. von http://www.worldtimeserver.com.
Jetzt einstellen	Wenn Sie hierauf klicken, werden das Datum und die UTC-Zeit, die Sie in dieser Zeile ausgewählt haben, übernommen.
Client-Zeit	Zeigt die Zeit entsprechend dem Client-Computer an, von dem aus Ihr Browser derzeit mit der Appliance verbunden ist.
Appliance mit Client synchronisieren	Bei Auswahl übernimmt die Zeit unter **Appliance-Zeit (UTC)** sofort den Wert aus **Client-Zeit**. Sie können dieses Kontrollkästchen als Alternative verwenden, um manuell die **Appliance-Zeit (UTC)** einzustellen. Die Appliance errechnet die UTC-Zeit basierend auf der Zeitzone, die sie im Client-Browser findet. Stellen Sie sicher, dass der Client-Computer Sommer- und Winterzeit berücksichtigt. Um die Einstellung in Microsoft Windows zu finden, klicken Sie mit der rechten Maustaste in die untere rechte Ecke des Bildschirms.
NTP aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten von einem angegebenen Server oder einem Netzwerk-Broadcast. NTP synchronisiert die Uhrzeiten unter den Geräten in einem Netzwerk. Einige Internet-Dienstanbieter bieten einen Uhrzeitdienst an. Da NTP-Nachrichten nicht häufig versendet werden, beeinträchtigen sie die Leistung der Appliance nicht wesentlich.
NTP-Client-Broadcasts aktivieren	Wenn ausgewählt, akzeptiert NTP Nachrichten nur von Netzwerk-Broadcasts. Diese Methode ist hilfreich, wenn das Netzwerk ausgelastet ist, aber anderen Geräten im Netzwerk vertrauen muss. Wenn diese Option nicht ausgewählt ist, akzeptiert NTP Nachrichten nur von Servern, die in der Liste angegeben sind.
NTP-Server	Zeigt die Netzwerkadresse oder einen Domänennamen eines oder mehrerer NTP-Server an, die die Appliance verwendet. Z. B. time.nist.gov. Wenn Sie mehrere Server angeben, prüft die Appliance jede NTP-Nachricht, um die richtige Uhrzeit zu bestimmen.
Neuer Server	Geben Sie die IP-Adresse eines neuen NTP-Servers ein.

Seite "Kennwort" (Setup im Modus 'Nur Verschlüsselung')

Geben Sie ein Kennwort für die Appliance an.



Ein sicheres Kennwort besteht aus Buchstaben und Ziffern. Sie können bis zu 15 Zeichen eingeben.

Option	Beschreibung
Benutzer-ID	Diese lautet **admin**. Sie können später weitere Benutzer hinzufügen.
Aktuelles Kennwort	Das bestehende Kennwort. Das ursprüngliche Standardkennwort lautet **password**. Ändern Sie das Kennwort baldmöglichst, damit Ihre Appliance geschützt bleibt.
Neues Kennwort/Neues Kennwort bestätigen	Gibt das neue Kennwort an. Sie müssen das neue Kennwort zweimal eingeben, um es zu bestätigen.

Seite "Zusammenfassung" (Setup im Modus 'Nur Verschlüsselung')

Zeigen Sie eine Zusammenfassung der Einstellungen an, die Sie für Netzwerkverbindungen und das Scannen des E-Mail-Verkehrs vorgenommen haben.

Wenn Sie einen Wert ändern möchten, klicken Sie auf den entsprechenden blauen Link, um die Seite anzuzeigen, auf der Sie den Wert ursprünglich eingegeben haben.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird der Setup-Assistent abgeschlossen.

Verwenden Sie die hier angezeigte IP-Adresse, um die Benutzeroberfläche aufzurufen. Beispiel: *https://192.168.200.10*. Die Adresse beginnt mit https und nicht mit http.



Wenn Sie Ihr McAfee® Email Gateway für Secure Web Mail konfiguriert haben, müssen Sie auf die Appliance über den Port 10443 zugreifen. Im oben angegebenen Beispiel würden Sie demzufolge *https://192.168.200.10:10443* eingeben.

Wenn Sie sich zum ersten Mal bei der Benutzeroberfläche anmelden, geben Sie den Benutzernamen **admin** und das Kennwort ein, das Sie auf der Seite **Kennwort** angegeben haben.

Tabelle 3-4 Grundlegende Einstellungen

Option	Beschreibung
✔	Der Wert entspricht bewährten Praktiken.
⚠	Der Wert ist wahrscheinlich nicht korrekt. Er ist zwar gültig, entspricht aber nicht bewährten Praktiken. Prüfen Sie den Wert, bevor Sie fortfahren.
–	Es wurde kein Wert festgelegt. Der vorgegebene Standardwert wurde nicht geändert. Prüfen Sie den Wert, bevor Sie fortfahren.

4 Vorstellung des Dashboards

In diesem Abschnitt wird die Seite "Dashboard" beschrieben und erläutert, wie ihre Voreinstellungen bearbeitet werden.

Das Dashboard

Das Dashboard bietet eine Zusammenfassung der Aktivitäten der Appliance.



Dashboard

Von dieser Seite aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern.

Auf einer Cluster-Master-Appliance verwenden Sie diese Seite auch, um eine Übersicht der Aktivitäten im Appliance-Cluster anzuzeigen.

Vorteile der Verwendung des Dashboards

Das Dashboard bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Appliance-Aktivitäten mithilfe verschiedener Portlets ansehen können.



Abbildung 4-1 Dashboard-Portlets

In einigen Portlets werden Grafiken angezeigt, die die Appliance-Aktivität in den folgenden Zeiträumen darstellen:

- 1 Stunde
- 1 Tag (Standard)
- 1 Woche
- 2 Wochen
- 4 Wochen

Im Dashboard können Sie einige Änderungen an den angezeigten Informationen und Diagrammen vornehmen:

- Vergrößern und Verkleinern der Portlet-Daten mithilfe der Symbole und rechts oben im Portlet
- Anzeige detaillierterer Daten mithilfe der Symbole und
- Eine Statusanzeige gibt an, ob das Element Aufmerksamkeit erfordert:
  - – **Fehlerfrei**. Die ausgewiesenen Elemente funktionieren normal.
  - – **Erfordert sofortige Aufmerksamkeit**. Ein kritischer Schwellenwert wurde überschritten.
  - – **Deaktiviert**. Der Dienst ist nicht aktiviert.

- Verwenden Sie und , um auf einer Zeitachse in Informationen herein- und herauszuzoomen. Es kommt zu einer kurzen Verzögerung, während die Ansicht aktualisiert wird. Standardmäßig zeigt das Dashboard Daten für den vorherigen Tag an.
- Verschieben eines Portlets an eine andere Stelle auf dem Dashboard
- Doppelklicken Sie auf die obere Leiste eines Portlets, um es auf den oberen Bereich des Dashboards zu vergrößern.
- Legen Sie eigene Warnhinweis- und Warnungsschwellenwerte zum Auslösen von Ereignissen fest. Markieren Sie dazu das Element, und klicken Sie darauf, bearbeiten Sie die Felder "Warnhinweisschwellenwert" und "Warnungsschwellenwert", und klicken Sie auf **Speichern**. Wenn das Element den von Ihnen festgelegten Schwellenwert überschreitet, wird ein Ereignis ausgelöst.



Abhängig von dem Browser, der zum Anzeigen der Benutzeroberfläche von McAfee Email Gateway verwendet wird, speichert das Dashboard den aktuellen Status jedes Portlets (ob es vergrößert oder verkleinert ist und ob Sie die Anzeige bestimmter Daten geöffnet haben) und versucht, die entsprechende Ansicht wiederherzustellen, wenn Sie zu einer anderen Seite in der Benutzeroberfläche navigieren und anschließend innerhalb derselben Browsersitzung zum Dashboard zurückkehren.

Bereiche der Seite "Dashboard"

In diesem Thema werden die Bereiche des Dashboards in der Benutzeroberfläche Ihres E-Mail-Gateways behandelt.

Option	Beschreibung
E-Mail-Erkennungen und **Web-Erkennungen**	Zeigt die Anzahl der Erkennungen unter jedem Protokoll an. Klicken Sie auf **Bearbeiten**, um die Ansicht in diesem Fenster zu ändern. Obwohl Sie festlegen können, dass zu einem Protokoll keine Informationen angezeigt werden, scannt die Appliance den Verkehr weiterhin.
Systemstatus	Zeigt den Status wichtiger Komponenten an und ermöglicht Ihnen, Änderungen an den Einstellungen von empfohlenen Systemkonfigurationsänderungen vorzunehmen: • Bei **Aktualisierungen** zeigt ein grünes Häkchen, dass die Komponenten automatisch aktualisiert werden. Wenn Sie eine manuelle Aktualisierung vornehmen möchten, klicken Sie auf den blauen Link. • Für andere Komponenten gibt ein grünes Häkchen an, dass die Komponente innerhalb akzeptabler Grenzwerte betrieben wird. Weiterführende Informationen erhalten Sie, wenn Sie auf die blauen Links klicken. • Sie können die Stufen anpassen, bei denen die Warnhinweissymbole angezeigt werden, und ändern, was im Dialogfeld mit den empfohlenen Konfigurationsänderungen angezeigt wird, indem Sie auf **Bearbeiten** klicken.
Aktuelle Erkennungsraten	Zeigt mithilfe von Symbolen den Status wichtiger Erkennungen der Appliance an.
Netzwerk	Zeigt die Anzahl der Verbindungen unter jedem Protokoll an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** abwählen können, wickelt die Appliance den Verkehr weiterhin ab.
E-Mail-Warteschlangen	Zeigt mithilfe von Symbolen die Anzahl der Elemente und die Anzahl der Empfänger für jedes Element in den Warteschlangen "In der Warteschlange", "Isoliert" und "Anfragen für Entlassen aus Quarantäne" an, die von der Appliance verwaltet werden. Wenn Sie auf die Seiten wechseln möchten, auf denen die Warteschlangen verwaltet werden, klicken Sie auf die blauen Links. Wenn Sie die E-Mails in den Warteschlangen schnell durchsuchen möchten, klicken Sie auf **Schnellsuche**.

Option	Beschreibung
Scan-Richtlinien	Zeigt eine Liste der von der Appliance eingesetzten Richtlinien an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** abwählen können, wendet die Appliance weiterhin Richtlinien auf den Verkehr an. Wenn Sie die Scan-Richtlinien anzeigen oder weitere Richtlinien hinzufügen möchten, klicken Sie auf die blauen Links.
Tasks	Zeigt eine Liste häufiger Aufgaben an. Wenn Sie Aufgaben entfernen oder neu organisieren möchten, klicken Sie auf **Bearbeiten**.
Lastenausgleich	Auf einer Master-Cluster-Appliance wird der Status des Appliance-Clusters angezeigt. Um die Einstellungen der Anzeige zu ändern, klicken Sie auf **Bearbeiten**.
Diagramme...	Zeigt Diagramme an, die die zeitliche Aktivität der Appliance darstellen. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** abwählen können, überwacht die Appliance den Verkehr weiterhin.

5 Testen der Konfiguration

Diese Informationen beschreiben, wie Sie testen können, ob die Appliance nach der Installation ordnungsgemäß funktioniert.

Inhalt

Vorgehensweise – Testen der Verbindung

Gehen Sie wie nachfolgend beschrieben vor, um die grundlegende Verbindungsfähigkeit zu bestätigen.

Das McAfee Email Gateway prüft, ob es mit dem Gateway kommunizieren und Server sowie DNS-Server aktualisieren kann. Außerdem wird überprüft, ob der Name der Appliance und der Name der Domäne gültig sind.

Vorgehensweise

1. Wählen Sie in der Navigationsleiste die Option **Fehlerbehebung**, oder wählen Sie im Dashboard im Bereich **Tasks** die Option **Systemtests ausführen**.
2. Wählen Sie die Registerkarte **Tests**.
3. Klicken Sie auf **Tests starten**.

Jeder Test sollte positiv beendet werden.

Vorgehensweise – Die DAT-Dateien aktualisieren

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass das McAfee Email Gateway über die aktuellsten Erkennungsdefinitionsdateien (DAT) verfügt. Es wird empfohlen, dass Sie diese aktualisieren, bevor Sie die Scan-Optionen konfigurieren.

Im Rahmen der Verwendung des McAfee Email Gateway können Sie einzelne Arten von Definitionsdateien aktualisieren sowie die standardmäßig geplanten Aktualisierungen an Ihre Anforderungen anpassen.

Vorgehensweise

1. Wählen Sie **System** | **Komponentenverwaltung** | **Aktualisierungsstatus**.
2. Klicken Sie zum Aktualisieren des Antiviren-Moduls und der Antiviren-Datenbank auf **Jetzt aktualisieren**.

   Für die Überprüfung, ob das Update korrekt angewendet wurde, öffnen Sie das Portlet **Dienste** im Dashboard, und erweitern Sie den Status für **Aktualisierungen**. Die Antiviren-Komponenten haben einen grünen Status.

Vorgehensweise – Testen von E-Mail-Verkehr und Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob der E-Mail-Verkehr erfolgreich durch das McAfee Email Gateway geleitet wird und ob dabei Gefahren ordnungsgemäß identifiziert werden. Wir verwenden die EICAR-Testdatei, eine harmlose Datei, die eine Virenerkennung auslöst.

Vorgehensweise

1. Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.
2. Sehen Sie sich im Dashboard die Bereiche mit den Erkennungen an. Aus der Liste für das Protokoll, das Sie zum Versenden der Nachricht verwendet haben, sollte hervorgehen, dass eine Nachricht empfangen wurde.
3. Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen:

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
4. Speichern Sie die Datei unter dem Namen EICAR.COM.
5. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.
6. Kehren Sie zum Dashboard zurück, und sehen Sie sich die Bereiche mit den Erkennungen an. Sie sollten sehen, dass ein Virus erkannt wurde.
7. Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.

Vorgehensweise – Testen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um einen *General Test mail for Unsolicited Bulk Email* (Allgemeiner Test auf unerwünschte Bulk-E-Mails, GTUBE) auszuführen, mit dem geprüft wird, ob das McAfee Email Gateway eingehende Spam-Mail erkennt.

Vorgehensweise

1. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.
2. Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:

   XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

   Achten Sie darauf, dass der Text keine Zeilenumbrüche enthält.

3. Senden Sie die neue E-Mail an eine interne Posteingangsadresse.

   Das Gerät scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.

   Nähere Informationen zum GTUBE-Test finden Sie unter http://spamassassin.apache.org/tests.html.

6 Erkunden der Funktionen der Appliance

Diese Informationen enthalten Vorgehensweisen zur Demonstration der Scan-Funktion der McAfee Email Gateway Virtual Appliance 7.0. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Einführung in die Richtlinien

Die Appliance verwendet Richtlinien zur Beschreibung der Aktionen, die die Appliance bei Bedrohung durch Viren, Spam, unerwünschte Dateien und Verlust kritischer Informationen ausführen muss.



E-Mail | E-Mail-Richtlinien

Richtlinien sind Sammlungen von Regeln oder Einstellungen, die auf bestimmte Arten von Datenverkehr oder auf Benutzergruppen angewendet werden können.

Verschlüsselung

Auf den Seiten **Verschlüsselung** können Sie McAfee Email Gateway für die Verwendung unterstützter Verschlüsselungsverfahren konfigurieren, damit E-Mail-Nachrichten sicher zugestellt werden.



E-Mail | Verschlüsselung

Das McAfee Email Gateway umfasst mehrere Verschlüsselungs-Methoden und kann dafür eingerichtet werden, anderen Scan-Funktionen Verschlüsselungsdienste zur Verfügung zu stellen. Es kann jedoch auch als reiner Verschlüsselung-Server nur für die Verschlüsselung von E-Mails verwendet werden.

Vorgehensweise – Verschlüsseln des gesamten E-Mail-Verkehrs mit einem bestimmten Kunden

Eine häufige Art der Nutzung von Verschlüsselungsfunktionen besteht in der Konfiguration einer Richtlinie, die festlegt, dass die Verschlüsselung nur für E-Mail-Nachrichten an einen bestimmten Kunden verwendet werden soll.

Die folgenden Vorgehensweisen zeigen auf, wie das McAfee Email Gateway so konfiguriert wird, dass alle E-Mail-Nachrichten, die an einen bestimmten Kunden gerichtet sind, verschlüsselt gesendet werden.

Vorgehensweise – Erstellen einer neuen Richtlinie

Erfahren Sie, wie Sie eine neue Scan-Richtlinie erstellen können.

Ihre Appliance scannt die über sie versendeten E-Mail-Nachrichten anhand der von Ihnen erstellten Richtlinien. Sie können mehrere Richtlinien erstellen, um zu steuern, wie unterschiedliche Benutzer E-Mail verwenden, oder um verschiedene Aktionen anzugeben, die abhängig von verschiedenen Bedingungen ausgeführt werden sollen.

Vorgehensweise

1. Klicken Sie auf **E-Mail** | **E-Mail-Richtlinien** | **Scan-Richtlinien**.
2. Wählen Sie das erforderliche Protokoll aus, indem Sie die Schritte unter *Vorgehensweise – Anzeigen der Richtlinien für SMTP, POP3 bzw. McAfee Secure Web Mail* ausführen.
3. Klicken Sie auf **Richtlinie hinzufügen...**
4. Geben Sie auf der Seite **Scan-Richtlinien – Neue Richtlinie** folgende Informationen an:
   a. Einen Namen für die Richtlinie.
   b. Eine optionale Beschreibung für die neue Richtlinie.
   c. Woher sich die Einstellungen der neuen Richtlinie ableiten.

      Wenn Sie bereits eine ähnliche Richtlinie eingerichtet haben, wählen Sie diese aus, um deren Einstellungen in die neue Richtlinie zu übernehmen.

   d. Wählen Sie aus, ob die Richtlinie auf ein- oder ausgehenden E-Mail-Verkehr angewendet werden soll. (Nur SMTP)
   e. Wählen Sie die erforderliche **Übereinstimmungs-Logik** für die Richtlinie aus.
   f. Wählen Sie den Regeltyp aus, wählen Sie, wie die Regel übereinstimmen sollte, und wählen Sie den den Wert aus, gegen den die Regel testet.
   g. Falls erforderlich, fügen Sie zusätzliche Regeln hinzu, und verwenden Sie die Schaltflächen ⇧ und ⇩, um die Regeln in die richtige Reihenfolge zu bringen.
5. Klicken Sie auf **OK**.

Die neue Richtlinie wird an den Anfang der Richtlinienliste gesetzt.

Vorgehensweise – Konfigurieren der Verschlüsselungseinstellungen

Konfigurieren Sie das McAfee Email Gateway für die Verwendung von Verschlüsselung.

Vorgehensweise

1. Klicken Sie auf **E-Mail** | **Verschlüsselung** | **Secure Web Mail** | **Grundlegende Einstellungen**.
2. Wählen Sie **Secure Web Mail-Client aktivieren**.
3. Klicken Sie auf **E-Mail** | **Verschlüsselung** | **Secure Web Mail** | **Benutzerkontoeinstellungen**.

   Empfänger werden automatisch angemeldet und erhalten eine digital signierte Benachrichtigung im HTML-Format. Der Administrator wählt, ob eine Push- und/oder eine Pull-Verschlüsselung vorgenommen wird.

4. Klicken Sie auf **E-Mail** | **Verschlüsselung** | **Secure Web Mail** | **Kennwortverwaltung**.

   Die minimale Kennwortlänge beträgt acht Zeichen. Das Kennwort läuft nach 365 Tagen ab.

Vorgehensweise – Aktivieren der Verschlüsselung in der E-Mail-Richtlinie

Aktivieren Sie die erforderlichen Verschlüsselungsfunktionen im McAfee Email Gateway.

Vorgehensweise

1. Klicken Sie auf **E-Mail** | **E-Mail-Richtlinien** | **Compliance**.
2. Klicken Sie auf **Compliance aktivieren**, und wählen Sie **Neue Regel aus Vorlage erstellen**.
3. Suchen Sie die Regel **HIPAA-Compliance**, und wählen Sie sie aus.
4. Klicken Sie auf **Weiter**, um jeweils zur nächsten Assistentenseite zu gelangen.
5. Wählen Sie als primäre Aktion "Durchlassen (Überwachen)".
6. Wählen Sie unter "Und auch" die Option **Nachricht verschlüsselt zustellen**.
7. Klicken Sie auf **Fertigstellen**, und klicken Sie dann auf **OK**, um das Dialogfeld zu schließen.
8. Klicken Sie auf **E-Mail** | **E-Mail-Richtlinien** | **Richtlinienoptionen** | **Verschlüsselung**.
9. Wählen Sie unter **Verschlüsselungszeitpunkt** die Option **Nur wenn von einer Scan-Aktion ausgelöst**.
10. Wählen Sie unter **Optionen zur integrierten Verschlüsselung** die Option **Secure Web Mail**, und klicken Sie auf **OK**.
11. Übernehmen Sie die Änderungen.

Vorgehensweise – Erkennen von isolierten E-Mail-Nachrichten

Gehen Sie wie nachfolgend beschrieben vor, um nach E-Mails zu suchen, die von Ihrer McAfee Email Gateway Appliance isoliert wurden.

So zeigen Sie eine Liste aller isolierten Nachrichten an:

Vorgehensweise

1. Klicken Sie auf **Berichte** | **Nachrichtensuche**.
2. Wählen Sie **Isoliert** in der Dropdown-Liste **Nachrichtenstatus** aus.
3. Klicken Sie auf **Suchen/Aktualisieren**.

Alle isolierten Nachrichten werden im unteren Bereich der Seite angezeigt.

Vorgehensweise – Eingrenzen der Suche

Sie können die Suche nach isolierten E-Mails weiter eingrenzen, sodass nur Nachrichten angezeigt werden, die aufgrund von bestimmten Auslösern isoliert wurden. Gehen Sie wie folgt vor, um in diesem Beispiel die E-Mails zu finden, die aufgrund von Compliance-Problemen in Quarantäne verschoben wurden:

Vorgehensweise

1. Führen Sie die unter *Vorgehensweise – Ermitteln, welche E-Mails isoliert sind* beschriebenen Schritte aus.
2. Wählen Sie **Compliance** in der Dropdown-Liste **Kategorie** aus.
3. Klicken Sie auf **Suchen/Aktualisieren**.

Der untere Bereich des Bildschirms wird aktualisiert, um nur die Nachrichten anzuzeigen, die aufgrund von Compliance-Problemen isoliert wurden.

Vorgehensweise – Anzeigen einer bestimmten E-Mail-Nachricht

Sie können den Inhalt einer isolierten E-Mail sehen.

Vorgehensweise

1. Führen Sie die Schritte unter *Vorgehensweise – Eingrenzen der Suche* aus.
2. Aktivieren Sie links auf der Seite das Kontrollkästchen, um die entsprechende isolierte Nachricht auszuwählen.
3. Klicken Sie auf **Nachricht anzeigen**.

Die ausgewählte Nachricht wird in einem neuen Fenster angezeigt. In diesem Fenster können Sie den Inhalt der E-Mail lesen. Außerdem können Sie alternativ die detaillierten Informationen des E-Mail-Headers anzeigen. Sobald Sie die Nachricht gelesen haben, können Sie weitere Aktionen für die E-Mail auswählen, indem Sie auf die entsprechenden Schaltflächen klicken.

Vorgehensweise – Freigeben einer isolierten E-Mail-Nachricht

Nachdem Sie die isolierte E-Mail-Nachricht gesehen haben, möchten Sie möglicherweise die Nachricht aus der Quarantäne freigeben. Gehen Sie dazu folgendermaßen vor.

So entlassen Sie eine ausgewählte Nachricht aus der Quarantäne

Vorgehensweise

1. Führen Sie die Schritte unter *Vorgehensweise – Anzeigen einer bestimmten E-Mail-Nachricht* aus.
2. Klicken Sie auf **Ausgewählte Elemente aus Quarantäne entlassen**.

Die ausgewählte E-Mail wird aus der Quarantäne entlassen.



E-Mails mit infiziertem Inhalt können nicht aus der Quarantäne entlassen werden, da dies Schäden auf Ihren Systemen verursachen könnte.

Compliance-Einstellungen

Über diese Seite können Sie Compliance-Regeln erstellen und verwalten.



E-Mail | E-Mail-Richtlinien | Compliance | Compliance

Vorteile der Compliance-Einstellungen

Verwenden Sie Compliance-Scans zur Unterstützung der Compliance mit gesetzlichen und betrieblichen Auflagen. Sie können aus einer Bibliothek aus vordefinierten Compliance-Regeln wählen oder eigene Regeln und Wörterbücher für Ihr Unternehmen erstellen.

Compliance-Regeln können hinsichtlich ihrer Komplexität von einem einfachen Auslöser bei der Erkennung eines einzelnen Begriffs in einem Wörterbuch bis hin zum Aufbauen auf und Kombinieren von faktorbasierten Wörterbüchern variieren, die nur auslösen, wenn ein bestimmter Schwellenwert erreicht wird. Mithilfe der erweiterten Funktionen von Compliance-Regeln können Wörterbücher mit den logischen Operationen *eines von*, *alle von* oder *außer* kombiniert werden.

Vorgehensweise – Beschränken des Faktorbeitrags eines Wörterbuchbegriffs

Gehen Sie wie nachfolgend beschrieben vor, um den Faktorbeitrag eines Wörterbuchbegriffs zu beschränken.

> **Bevor Sie beginnen**
>
> Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch **Vergütung und Leistungen**.

Sie können beschränken, wie oft ein Begriff zum Gesamtfaktor beitragen kann.

Wenn beispielsweise "Testbegriff" in einem Wörterbuch den Faktor 10 hat und fünfmal in einer E-Mail erkannt wird, wird 50 zum Gesamtfaktor addiert. Alternativ können Sie eine Beschränkung festlegen, sodass beispielsweise nur zwei Vorkommnisse zum Gesamtwert beitragen, indem Sie für "Max. Begriffsanzahl" den Wert "2" angeben.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten, und klicken Sie anschließend auf das Symbol **Bearbeiten** neben dem Wörterbuch, dessen Faktor Sie ändern möchten.
3. Geben Sie unter **Max. Begriffsanzahl** die maximale Anzahl an Vorkommnissen eines Begriffs an, die zum Gesamtfaktor beitragen sollen.

Vorgehensweise – Bearbeiten des einer vorhandenen Regel zugewiesenen Schwellenwerts

Gehen Sie wie nachfolgend beschrieben vor, um den Schwellenwert zu bearbeiten, der einer vorhandenen Regel zugeordnet ist.

> **Bevor Sie beginnen**
>
> Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch **Vergütung und Leistungen**.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten, und wählen Sie anschließend das Symbol **Bearbeiten** neben dem Wörterbuch aus, dessen Faktor Sie ändern möchten.
3. Geben Sie unter "Schwellenwert für Wörterbuch" den Faktor ein, bei dem die Regel ausgelöst werden soll, und klicken Sie auf **OK**.

Vorgehensweise – Definieren einer Regel zum Überwachen oder Blockieren bei Erreichen eines Schwellenwerts

Bei faktorbasierten Wörterbüchern kann es sinnvoll sein, Auslöser zu überwachen, die einen niedrigen Schwellenwert erreichen, und die E-Mails nur zu blockieren, wenn ein hoher Schwellenwert erreicht wird.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Compliance**.
2. Klicken Sie auf **Neue Regel erstellen**, geben Sie einen Namen für die Regel ein, beispielsweise `Unzufriedenheit - Niedrig`, und klicken Sie auf **Weiter**.
3. Wählen Sie das Wörterbuch "Unzufriedenheit" aus, und geben Sie unter **Schwelle** den Wert `20` ein.
4. Klicken Sie auf **Weiter** und anschließend erneut auf **Weiter**.
5. Akzeptieren Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Standardaktion.
6. Klicken Sie auf **Fertig stellen**.
7. Wiederholen Sie die Schritte 2 bis 4, um eine weitere neue Regel zu erstellen. Nennen Sie diese jedoch `Unzufriedenheit - Hoch`, und weisen Sie ihr den Schwellenwert 40 zu.
8. Wählen Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Option **Verbindung verweigern (Blockieren)** aus.
9. Klicken Sie auf **Fertig stellen**.
10. Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Hinzufügen eines Wörterbuchs zu einer Regel

Gehen Sie wie folgt vor, um ein neues Wörterbuch zu einer vorhandenen Regel hinzuzufügen.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Compliance**.
2. Erweitern Sie die Regel, die Sie bearbeiten möchten.
3. Wählen Sie **Wörterbuch hinzufügen**.
4. Wählen Sie das neue Wörterbuch aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

Vorgehensweise – Erstellen einer komplexen benutzerdefinierten Regel

Gehen Sie wie nachfolgend beschrieben vor, um eine komplexe Regel zu erstellen, die auslöst, wenn sowohl Wörterbuch A als auch Wörterbuch B erkannt werden, jedoch nicht, wenn darüber hinaus auch Wörterbuch C erkannt wird.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Scan-Richtlinien** , und wählen Sie **Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, um den Assistent für die Regelerstellung zu öffnen.
4. Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.
5. Wählen Sie zwei Wörterbücher aus, die in die Regel aufgenommen werden sollen, und klicken Sie auf **Weiter**.
6. Wählen Sie in der Ausschlussliste ein Wörterbuch aus, das Sie von der Regel ausschließen möchten.
7. Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die Regel ausgelöst wird.
8. Wählen Sie im Dropdown-Feld **Und bedingt** die Option **Alle** aus, und klicken Sie auf **Fertig stellen**.

Vorgehensweise – Erstellen einer einfachen benutzerdefinierten Regel

Gehen Sie wie nachfolgend beschrieben vor, um eine einfache benutzerdefinierte Regel zu erstellen, die Nachrichten blockiert, die Sozialversicherungsnummern enthalten.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, um den Assistent für die Regelerstellung zu öffnen.
4. Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.
5. Geben Sie im Suchfeld `sozial` ein.
6. Wählen Sie das Wörterbuch "Sozialversicherungsnummer" aus, und klicken Sie zweimal auf **Weiter**.
7. Wählen Sie die Aktion **Verbindung verweigern (Blockieren)** aus, und klicken Sie auf **Fertig stellen**.

Vorgehensweise – Blockieren von Nachrichten, die gegen eine Richtlinie verstoßen

Gehen Sie wie nachfolgend beschrieben vor, um E-Mail-Nachrichten zu blockieren, die die Richtlinie "Bedrohliche Sprache" verletzen.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Compliance**.
2. Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel aus Vorlage erstellen**, um den Assistenten für die Regelerstellung zu öffnen.
4. Wählen Sie die Richtlinie **Zulässige Nutzung - Bedrohliche Sprache** aus, und klicken Sie auf **Weiter**.
5. Sie können den Namen der Regel optional ändern. Klicken Sie anschließend auf **Weiter**.
6. Ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **Fertig stellen**.
7. Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

Data Loss Prevention-Einstellungen

Auf dieser Seite können Sie eine Richtlinie erstellen, die Data Loss Prevention-Aktionen für die Kategorien der registrierten Dokumente zuweist.


E-Mail | **E-Mail-Richtlinien** | **Compliance** | **Data Loss Prevention**

Vorteile des Einsatzes von Data Loss Prevention (DLP)

Mit der Data Loss Prevention-Funktion können Sie den Fluss kritischer Informationen beschränken, die in E-Mail-Nachrichten per SMTP über die Appliance gesendet werden. Sie können beispielsweise die Übertragung eines kritischen Dokuments, wie z. B. eines Finanzberichts, blockieren, das an eine Adresse außerhalb Ihres Unternehmens gesendet werden soll. Die Erkennung erfolgt, sobald das Originaldokument als E-Mail-Anhang oder als Textausschnitt aus dem Originaldokument versendet wird.

Die DLP-Konfiguration erfolgt in zwei Phasen:

- Registrierung der Dokumente, die geschützt werden sollen.
- Aktivieren der DLP-Richtlinie und Kontrollieren der Erkennung (dieses Thema)



Wenn ein hochgeladenes registriertes Dokument eingebettete Dokumente enthält, wird von deren Inhalt ebenfalls ein Fingerabdruck angelegt. Wenn später während eines Scans der Übereinstimmungsprozentsatz berechnet wird, wird der kombinierte Inhalt verwendet. Wenn eingebettete Dokumente separat behandelt werden sollen, müssen sie separat registriert werden.

Vorgehensweise – Verhindern, dass ein vertrauliches Dokument gesendet wird

Im Folgenden erfahren Sie, wie Sie verhindern, dass vertrauliche Finanzdokumente aus Ihrem Unternehmen heraus gesendet werden.

Bevor Sie beginnen

In diesem Beispiel wird davon ausgegangen, dass Sie bereits die Kategorie "Finanzen" erstellt haben.

Vorgehensweise

1. Wählen Sie **E-Mail | E-Mail-Richtlinien | Compliance | Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste "Regeln" angezeigt wird.
4. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **OK**.
5. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Blockieren des Versendens eines Dokumentabschnitts

Gehen Sie wie nachfolgend beschrieben vor, um zu verhindern, dass auch nur ein kleiner Abschnitt eines Dokuments aus Ihrem Unternehmen heraus gesendet wird.

Vorgehensweise

1. Wählen Sie **E-Mail | E-Mail-Richtlinien | Compliance | Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Aktivieren Sie die Einstellung für aufeinander folgende Signaturen, und geben Sie die Anzahl an aufeinander folgende Signaturen ein, bei der die DLP-Richtlinie eine Erkennung auslösen soll. Der Standardwert ist **10**.
4. Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste "Regeln" angezeigt wird.
5. Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Verbindung verweigern (Blockieren)**, und klicken Sie auf **OK**.
6. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Vorgehensweise – Ausschließen eines bestimmten Dokuments für eine Richtlinie

Gehen Sie wie nachfolgend beschrieben vor, um zu verhindern, dass ein bestimmtes Finanzdokument die DLP-Richtlinieneinstellungen auslöst.

Vorgehensweise

1. Wählen Sie **E-Mail** | **E-Mail-Richtlinien** | **Compliance** | **Data Loss Prevention**.
2. Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.
3. Klicken Sie auf **Dokumentausschluss erstellen**, wählen Sie das Dokument aus, das von dieser Richtlinie ignoriert werden soll, und klicken Sie auf **OK**.
4. Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

7 Zusätzliche Konfigurationsoptionen

Diese Informationen geben Ihnen einige Tipps zu bewährten Vorgehensweisen und stellen Ihnen einige erweiterte Konfigurationsoptionen vor.

Inhalt

Vorgehensweise – Upgrade auf Email Gateway Virtual Appliance 7.0

Gehen Sie wie nachfolgend beschrieben vor, um mithilfe des ISO-Images der Software ein Upgrade von Email and Web Security Virtual Appliance 5.6 oder Email Security Virtual Appliance 5.6 auf McAfee Email Gateway Virtual Appliance 7.0 durchzuführen.

Bevor Sie beginnen

Email and Web Security Virtual Appliance 5.6 oder Email Security Virtual Appliance 5.6 müssen bereits installiert sein.

Nachdem ein Betriebssystem auf einer virtuellen Appliance installiert wurde, startet die virtuelle Maschine immer zuerst direkt von der Festplatte. Um diese Funktion zu umgehen, müssen Sie die virtuelle Maschine herunterfahren und eine Startverzögerung beim Hochfahren konfigurieren, so dass Sie genügend Zeit haben, auf das **Boot**-Menü zuzugreifen und stattdessen das Starten über die Installations-CD zu veranlassen.

Vorgehensweise

1. Laden Sie die ISO-Upgrade-Datei für McAfee Email Gateway Virtual Appliance 7.0 von der McAfee-Download-Seite herunter, und extrahieren Sie sie.
2. Fahren Sie die virtuelle Appliance herunter.
   a. Melden Sie sich bei der Benutzeroberfläche der virtuellen Appliance an, und wählen Sie **System | Systemverwaltung | Systembefehle**.
   b. Geben Sie das Kennwort ein.
   c. Wählen Sie **Appliance beenden**.
3. Melden Sie sich beim VMware ESX-Server an, oder verwenden Sie den VMware Infrastructure Client bzw. den VMware vSphere Client, um sich beim VMware Virtual Center Server anzumelden.

4 Aktivieren Sie eine **Power-on-Boot**-Verzögerung, damit Sie ausreichend Zeit haben, die virtuelle Maschine von der CD aus starten zu lassen:

   a Wählen Sie die virtuelle Appliance in Liste **Inventory** (Inventar), und klicken Sie auf **Summary** (Zusammenfassung).

   b Wählen Sie **Edit Settings | Options | Boot Options** (Einstellungen bearbeiten | Optionen | Boot-Optionen).

   c Geben Sie unter **Power-on-Boot** (Power-on-Boot-Verzögerung) `10,000` in das Textfeld ein, und klicken Sie auf **OK**.

5 Schalten Sie die virtuelle Appliance ein.

6 Stellen Sie sicher, dass sich der Mauszeiger in der Konsole der virtuellen Appliance befindet. Drücken Sie anschließend die ESC-Taste, um das **Boot Menu** (Boot-Menü) zu öffnen.



Wählen Sie noch keine Optionen.

7 Ziehen Sie den Mauszeiger aus der Konsole, und wählen Sie **Connect CD/DVD1** (CD/DVD1 verbinden).

8 Gehen Sie zu dem Ordner, in den Sie die ISO-Datei für McAfee Email Gateway Virtual Appliance 7.0 heruntergeladen haben, und doppelklicken Sie auf **<McAfee-MEG 7.0-<Build-Nummer>.VMbuy.iso>**.

9 Wenn die ISO-Datei verbunden ist, klicken Sie erneut auf das Konsolenfenster. Wählen Sie **CD-ROM Drive** (CD-ROM-Laufwerk) aus, und drücken Sie die `EINGABE`-Taste.

10 Die virtuelle Appliance startet von der ISO-Datei.

11 Geben Sie **j** ein, um den Bedingungen der Endbenutzer-Lizenzvereinbarung zuzustimmen.

12 Wählen Sie die gewünschte Upgrade-Option, und drücken Sie die `Eingabetaste`, um das Upgrade durchzuführen.

13 Geben Sie **j** ein, um zu bestätigen, dass Sie fortfahren möchten.

Vorgehensweise – Ändern der standardmäßigen Aktionen zum Ausschalten und Zurücksetzen

Gehen Sie wie nachfolgend beschrieben vor, um die Aktionen zum **Ausschalten** und **Zurücksetzen** in VMware vSphere so zu ändern, dass die McAfee Email Gateway Virtual Appliance 7.0 heruntergefahren werden kann, ohne dass das Dateisystem der virtuellen Maschine beschädigt wird.

Vorgehensweise

1 Klicken Sie im **VMware vSphere Client** mit der rechten Maustaste auf McAfee Email Gateway Virtual Appliance 7.0, und wählen Sie **Edit Settings** (Einstellungen bearbeiten).

2 Wählen Sie die Registerkarte **Options** (Optionen), und wählen Sie **VMware Tools**.

3 Setzen Sie die Option neben dem roten Kästchen auf **Shut Down Guest** (Gast herunterfahren).

4 Setzen Sie die Option neben dem Symbol **Reset** (Zurücksetzen) (roter und grüner Pfeil) auf **Restart Guest** (Gast neu starten).

Vorgehensweise – Konfigurieren der Optionen zum Herunterfahren und Neustart

Gehen Sie wie nachfolgend beschrieben vor, um die McAfee Email Gateway Virtual Appliance 7.0 so zu konfigurieren, dass sie automatisch heruntergefahren und neu gestartet wird, wenn Sie VMware vSphere neu starten.

Vorgehensweise

1. Wählen Sie den vSphere-Host aus, und klicken Sie auf die Registerkarte **Configuration** (Konfiguration).
2. Wählen Sie **Virtual Machine Startup/Shutdown** (Start/Herunterfahren der virtuellen Maschine) im Feld "Software" aus, klicken Sie auf **Properties** (Eigenschaften), und führen Sie folgende Schritte aus:
   - Aktivieren Sie die Option **Allow virtual machines to start and stop automatically with the system** (Virtuellen Maschinen das automatische Starten und Anhalten mit dem System erlauben).
   - Ändern Sie die **Shutdown Action** (Aktion bei Herunterfahren) in **Guest Shutdown** (Gast herunterfahren).
3. Wählen Sie McAfee Email Gateway Virtual Appliance 7.0 in der Liste aus, und klicken Sie auf **Move Up** (Nach oben), bis sie an oberster Stelle in der Liste erscheint.
4. Klicken Sie auf **Bearbeiten**.
5. Wählen Sie unter **Virtual Machine Autostart Settings** (Autostart-Einstellungen für die virtuelle Maschine) im Feld **Shutdown Settings** (Einstellungen für Herunterfahren) die Option **Use specified settings** (Angegebene Einstellungen verwenden) aus, und wählen Sie dann **Guest Shutdown** (Gast herunterfahren) neben **Perform shutdown action** (Aktion zum Herunterfahren durchführen).
6. Klicken Sie zwei Mal auf **OK**, um das Konfigurationsfenster zu schließen.

Die virtuelle Appliance wird nun in der Liste unter der Überschrift **Automatic Startup** (Automatischer Start) angezeigt, und der Wert in der Spalte **Shutdown** (Herunterfahren) lautet **Shut down guest** (Gast herunterfahren).

Index

700-3349A15